SECURITY SUMMARY REPORT

Scorecard for Ovofinance

SecurityScorecard

Generated **March 18, 2022**
by Rawat Kulsirirut (rawat@nextwave.co.th), NextWave (Thailand)

C 74

Threat Indicators

F 51
NETWORK SECURITY
Detecting insecure network settings

A 100
DNS HEALTH
Detecting DNS insecure configurations and vulnerabilities

F 57
PATCHING CADENCE
Out of date company assets which may contain vulnerabilities or risks

D 69
ENDPOINT SECURITY
Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops

B 84
IP REPUTATION
Detecting suspicious activity, such as malware or spam, within your company network

A 100
APPLICATION SECURITY
Detecting common website application vulnerabilities

A 100
CUBIT SCORE
Proprietary algorithms checking for implementation of common security best practices

A 100
HACKER CHATTER
Monitoring hacker sites for chatter about your company

A 100
INFORMATION LEAK
Potentially confidential company information which may have been inadvertently leaked

A 100
SOCIAL ENGINEERING
Measuring company awareness to a social engineering or phishing attack

Industry Comparison:
Financial Services

ovofinance.com
industry average

VULNERABILITIES	MEASURE
Open Ports	74
Site Vulnerabilities	0
Malware Discovered	2
Leaked Information	0

SecurityScorecard

DETAILED REPORT

Scorecard for Ovofinance

Generated **March 18, 2022**
by Rawat Kulsirirut (rawat@nextwave.co.th), NextWave (Thailand)

About this report

This report is a point-in-time capture of this Scorecard as of 6:59:20 AM UTC, March 18, 2022. It should not be confused with a pen test result or a final assessment.

Get the full picture with SecurityScorecard

SecurityScorecard offers ongoing self-monitoring, history reports, CSV data exports, and more to help security teams protect their organizations. For full free access to your organization's Scorecard, create an account today at bit.ly/2P8okyb.

Learn more about SecurityScorecard at bit.ly/2xXNg4N today.

What is SecurityScorecard?

SecurityScorecard is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors. A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies[1]. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Learn more about SecurityScorecard's rating system at bit.ly/2zMLSmW.

[1] "New SecurityScorecard Research Can Help You Detect a Data Breach Before It Happens" (https://bit.ly/2yc0JVN)

Next Steps: Get to an A

1. Create an account

This file has a lot of detail but remember, it's only for one point in time. Create an account to get full free access to your organizaton's Scorecard along with continuous self-monitoring, history reports, CSV data exports, and more.

2. Validate your Digital Footprint

Once you have an account, review your company's Digital Footprint, the assets SecurityScorecard found as potentially attributable to your company, that affect the ratings in your Scorecard. Request removal or addition of IPs as needed.

3. Review issue findings

Investigate the contents of your Scorecard with your team(s). It's a win for your company's security posture when you identify loose ends of which you weren't aware.

4. Remediate issues, improve your score

Whether you've deployed a fix, found assets that don't belong to your company, or want to share information about compensating controls, you can let us know by remediating the identified finding(s) and submitting them for resolution approval. Resolutions are handled by our Support team, which will resolve any outstanding item within three business days. Remediate issues within the platform or email support@securityscorecard.com.

We're here to help

The SecurityScorecard platform is based on transparency and collaboration. Our Customer Reliability Support team provides remediation and resolution services at no charge and are happy to work with you and your customers to resolve any issues. If you need assistance at any stage, get in touch by emailing support@securityscorecard.io.

Scorecard Overview

C

Ovofinance

74 Security Score

DOMAIN: ovofinance.com

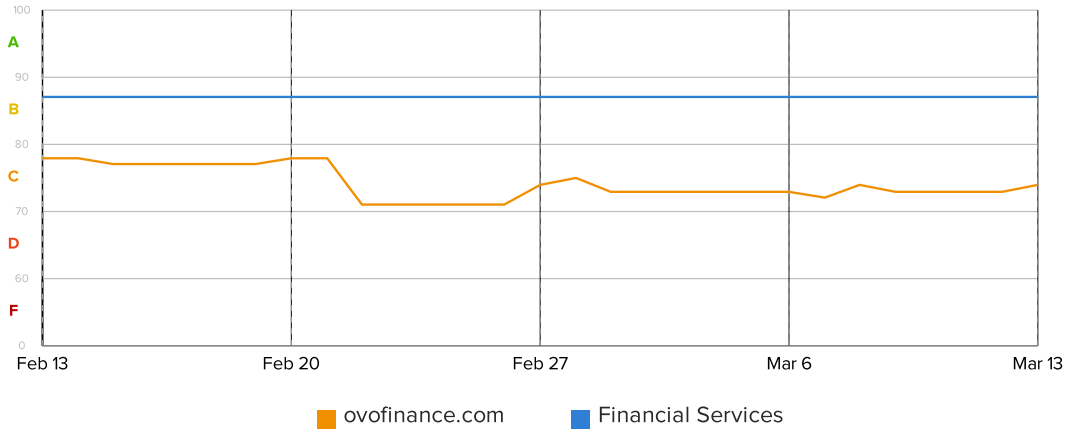
INDUSTRY: FINANCIAL SERVICES

Factors

A	100	APPLICATION SECURITY	0 ISSUES	B 84	IP REPUTATION	5 ISSUES
A	100	CUBIT SCORE	0 ISSUES	A 100	INFORMATION LEAK	0 ISSUES
A	100	DNS HEALTH	0 ISSUES	F 51	NETWORK SECURITY	22 ISSUES
D	69	ENDPOINT SECURITY	3 ISSUES	F 57	PATCHING CADENCE	9 ISSUES
A	100	HACKER CHATTER	0 ISSUES	A 100	SOCIAL ENGINEERING	1 ISSUE

30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open isues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.



Action Items

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Endpoint Security	!!!	-3.6	Outdated Web Browser Observed. An outdated web browser connected to a web server.
	!!!	-5.4	Outdated Operating System Observed. A web browser on an outdated operating system connected to a web server.
IP Reputation	!!!	-1.0	Malware Infection. Communications indicative of malware infections were observed over the last 30 days.
Network Security	!!!	-1.3	Industrial Control System Device Accessible. We observed an industrial control system (ICS) device publicly exposed.
	!!!	-1.9	SSL/TLS Service Supports Weak Protocol. A TLS service was observed supporting weak protocols.
	!!!	-0.7	SSH Software Supports Vulnerable Protocol. Server(s) observed running SSH software that support an SSH protocol lower than version 2.
	!!	-1.4	Certificate Is Self-Signed. Self-signed certificates prevent TLS clients from connecting to servers.
	!!	-0.3	Remote Access Service Observed. We observed a remote access service or device publicly exposed.
	!!	-1.2	TLS Service Supports Weak Cipher Suite. A TLS service was observed supporting weak cipher suites.
	!!	-1.2	Certificate Signed With Weak Algorithm. A certificate was observed that was signed with a weak algorithm.
	!!	-0.3	SSH Supports Weak MAC. A weak Message Authentication Code (MAC) algorithm has been detected.
	!!	-0.3	RDP Service Observed. We observed RDP, a remote access service, publicly exposed.
	!!	-1.4	Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers.
	!!	-0.3	PPTP Service Accessible. We observed a service running PPTP, an obsolete and insecure VPN-like protocol, publicly exposed.
	!!	-0.3	SSH Supports Weak Cipher. A weak cipher has been detected.
	!	-0.5	Certificate Without Revocation Control. A certificate was observed that did not contain either CRL or OCSP URLs.
	!	-0.3	FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed.
	!	-0.5	Certificate Lifetime Is Longer Than Best Practices. A certificate was observed with a validity period longer than dictated by the CAB forum's baseline requirements.
	!	-0.3	Telnet Service Observed. We observed Telnet, a remote access service, publicly exposed.
	!	-0.2	IP Camera Accessible. We observed an IP Camera, a video or image feed, publicly exposed.
Patching Cadence	!!!	-0.8	High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
	!!!	-1.1	High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 45 days after CVE was published.
	!!	-0.6	Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 90 days after CVE was published.
	!!	-0.5	Medium-Severity Vulnerability in Last Observation. We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.
	!	-0.2	Low Severity CVEs Patching Cadence. Low severity vulnerability seen network more than 120 days after CVE was published.
	!	-0.2	Low-Severity Vulnerability in Last Observation. We observed a low-severity vulnerability during our last scan, which may still be publicly exposed.

A 100 APPLICATION SECURITY

The Web Application Vulnerability module uses incoming threat intelligence from known exploitable conditions identified via: whitehat CVE databases, blackhat exploit databases, and sensitive findings indexed by major search engines. The module ingests data from multiple public data sets, third party feeds, and an internal proprietary indexing and aggregation engine.
The score determines the likelihood of an upcoming web application breach, and checks for any existing defacement code. Presence of vulnerable applications, outdated versions, and active defacements are used to calculate the overall grade.

HIGH SEVERITY

There are no High Severity Issues for Application Security

MEDIUM SEVERITY

There are no Medium Severity Issues for Application Security

LOW SEVERITY

There are no Low Severity Issues for Application Security

POSITIVE

There are no Positive Signals for Application Security

INFORMATIONAL

There are no Informational Signals for Application Security

No issues found

A 100 CUBIT SCORE

This proprietary module measures a variety of security issues that a company might have. For example, we check public threat intelligence databases for IP addresses that have been flagged. These misconfigurations may have high exploitability and could cause significant harm to the privacy of your data and infrastructure

HIGH SEVERITY

There are no High Severity Issues for Cubit Score

MEDIUM SEVERITY

There are no Medium Severity Issues for Cubit Score

LOW SEVERITY

There are no Low Severity Issues for Cubit Score

POSITIVE

There are no Positive Signals for Cubit Score

INFORMATIONAL

There are no Informational Signals for Cubit Score

No issues found

A 100 DNS HEALTH

This module measures the health and configuration of a company's DNS settings. It validates that no malicious events occurred in the passive DNS history of the company's network. It also helps validate that mail servers have proper protection in place to avoid spoofing. It also helps verify that DNS servers are configured correctly.

HIGH SEVERITY
There are no High Severity Issues for DNS Health

MEDIUM SEVERITY
There are no Medium Severity Issues for DNS Health

LOW SEVERITY
There are no Low Severity Issues for DNS Health

POSITIVE
There are no Positive Signals for DNS Health

INFORMATIONAL
There are no Informational Signals for DNS Health

No issues found

D 69 ENDPOINT SECURITY

The Endpoint Security Module tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins. The information gathered allows companies to identify outdated versions of these data points which can lead to client-side exploitation attacks.

HIGH SEVERITY

Outdated Web Browser Observed	3
Outdated Operating System Observed	6

MEDIUM SEVERITY

There are no Medium Severity Issues for Endpoint Security

LOW SEVERITY

There are no Low Severity Issues for Endpoint Security

POSITIVE

There are no Positive Signals for Endpoint Security

INFORMATIONAL

Browser Average Age Indicates Older Versions	40

Outdated Web Browser Observed

An outdated web browser connected to a web server.

-3.6 SCORE IMPACT

Description

The web is constantly evolving, using different languages, protocols, and file formats over time. Web browsers regularly release new versions, on time scales as short as every six weeks. These new versions frequently contain security and stability fixes.

When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated web browser was in use as described in the table below.

Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.

Recommendation

Update the web browsers in question. Enable automatic updates if available from your web browser vendor and permitted in your environment.

3 findings

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	EVIDENCE	LAST OBSERVED
Google	Chrome	90.0.4430.72	end of service	98.0.4758.102	2.192.4.182		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36	3/8/2022, 8:06:22 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	EVIDENCE	LAST OBSERVED
Google	Chrome	90.0.4430.72	end of service	98.0.4758.102	2.192.4.96		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36	3/7/2022, 11:29:05 AM
Google	Chrome	87.0.4280.141	end of service	98.0.4758.102	2.192.9.10		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 OverwolfClient/0.190.0.12	2/12/2022, 4:13:57 PM

Outdated Operating System Observed

-5.4 SCORE IMPACT

A web browser on an outdated operating system connected to a web server.

Description

When a web browser connects to a web server, it informs the server its platform and version information. This information assists the server in providing appropriate content. The information can also be recorded and aggregated to determine what platforms and browser versions are being used by hosts at various places on the Internet. Using such a data set, it was found that an outdated operating system was in use as described in the table below.
Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or NAT gateway with a single external IP will appear to be the source of an entire network full of corporate desktops.

Recommendation

Update affected device's operating system. Enable automatic updates if available from your software vendor and permitted in your environment. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

6 findings

MANUFACTURER	PRODUCT	VERSION	STATUS	SOURCE IP	PORTS	EVIDENCE	LAST OBSERVED
Microsoft	Windows 7	7	end of service	2.192.12.89		Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0	3/10/2022, 11:50:46 AM
Microsoft	Windows 7	7	end of service	2.192.11.181		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36	3/3/2022, 12:24:20 PM
Microsoft	Windows 7	7	end of service	2.192.4.184		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36	2/24/2022, 3:05:30 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	SOURCE IP	PORTS	EVIDENCE	LAST OBSERVED
Microsoft	Windows 7	7	end of service	2.192.7.185		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36	2/18/2022, 3:16:23 PM
Microsoft	Windows 7	7	end of service	2.192.11.114		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36	2/16/2022, 8:07:36 AM
Microsoft	Windows 7	7	end of service	2.192.6.154		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36	2/14/2022, 3:30:24 PM

Browser Average Age Indicates Older Versions

Our quantitative measurement of the adoption of latest browser versions indicates that out-of-date versions are in use at one or more of your IP addresses.

Description

The web is constantly evolving over time, using different languages, protocols, and file formats. Web browsers regularly release new versions with security and stability fixes. When a web browser connects to a web server, it informs the server about its operating software and browser version. This information helps the server provide appropriate content. It can also be recorded, aggregated, and used to determine what operating software and browser versions the hosts are using to connect to the internet. We analyze this data to determine average browser age, or how many browsers with out-of-date versions are in use at a given IP address, as described in the table below. This information indicates how diligent your organization is in keeping web browsers up to date. When a new major version is released, we denote the age of the latest version as 0, and we change the age of each preceding version by an increment of 1. So with a new release, the 0 version becomes 1, the 1 version becomes 2, and so on. Note that a single external IP address, such as those in the table below, may correspond to any number of internal hosts. For example, a company firewall or network address translation (NAT) gateway with a single external IP will appear to be the source of an entire network of corporate desktops.

Recommendation

Update the web browsers in question to the latest major release versions. Enable automatic updates if available from your web browser vendor and permitted in your environment.

40 findings

PRODUCT	AVERAGE VERSIONS BEHIND	SOURCE IP	LAST OBSERVED
Chrome	4	2.192.9.119	3/11/2022, 12:00:00 AM
Firefox		2.192.4.42	3/11/2022, 12:00:00 AM
Chrome		2.192.4.42	3/11/2022, 12:00:00 AM
Chrome		2.192.1.81	3/11/2022, 12:00:00 AM
Chrome		2.192.10.153	3/11/2022, 12:00:00 AM
Chrome		2.192.5.193	3/11/2022, 12:00:00 AM
Chrome		2.192.12.89	3/11/2022, 12:00:00 AM
Chrome		2.192.12.168	3/11/2022, 12:00:00 AM
Chrome		2.192.4.120	3/11/2022, 12:00:00 AM
Chrome		2.192.6.174	3/10/2022, 12:00:00 AM
Chrome	0.3333333333333333	2.192.0.185	3/10/2022, 12:00:00 AM

PRODUCT	AVERAGE VERSIONS BEHIND	SOURCE IP	LAST OBSERVED
Chrome	0.25	2.192.11.181	3/10/2022, 12:00:00 AM
Chrome		2.192.2.200	3/10/2022, 12:00:00 AM
Chrome	0.0833333358168602	2.192.5.51	3/10/2022, 12:00:00 AM
Firefox		2.192.12.89	3/10/2022, 12:00:00 AM
Chrome		2.192.0.252	3/10/2022, 12:00:00 AM
Chrome	1	2.192.1.15	3/9/2022, 12:00:00 AM
Chrome		2.192.0.208	3/9/2022, 12:00:00 AM
Chrome	0.5	2.192.1.0	3/9/2022, 12:00:00 AM
Chrome	4	2.192.4.182	3/9/2022, 12:00:00 AM
Chrome	1	2.192.7.245	3/9/2022, 12:00:00 AM
Firefox	1	2.192.3.127	3/9/2022, 12:00:00 AM
Chrome	1	2.192.1.55	3/8/2022, 12:00:00 AM
Chrome		2.192.1.158	3/8/2022, 12:00:00 AM
Chrome		2.192.5.79	3/7/2022, 12:00:00 AM
Chrome		2.192.6.201	3/7/2022, 12:00:00 AM
Chrome	1	2.192.11.31	3/7/2022, 12:00:00 AM
Chrome	1	2.192.6.0	3/7/2022, 12:00:00 AM
Chrome	1	2.192.10.160	3/7/2022, 12:00:00 AM
Chrome	1	2.192.0.111	3/7/2022, 12:00:00 AM
Chrome		2.192.3.133	3/7/2022, 12:00:00 AM
Chrome	4	2.192.4.96	3/7/2022, 12:00:00 AM
Chrome		2.192.2.0	3/7/2022, 12:00:00 AM
Chrome	1	2.192.6.18	3/6/2022, 12:00:00 AM
Chrome	1	2.192.5.224	3/6/2022, 12:00:00 AM
Chrome		2.192.5.209	3/6/2022, 12:00:00 AM
Chrome		2.192.5.214	3/5/2022, 12:00:00 AM
Opera	1	2.192.6.82	3/5/2022, 12:00:00 AM
Chrome		2.192.4.149	3/5/2022, 12:00:00 AM
Chrome	1	2.192.1.24	3/5/2022, 12:00:00 AM

A 100 HACKER CHATTER

The SecurityScorecard Hacker Chatter module is an automated collection and aggregation system for the analysis of multiple streams of underground hacker chatter. Forums, IRC, social networks, and other public repositories of hacker community discussions are continuously monitored, collected and aggregated in order to locate mentions of business names and websites. The Hacker Chatter score is an informational indicator ranking that is ranked based on the quantity of indicators that appear within the collection sensors.

HIGH SEVERITY

There are no High Severity Issues for Hacker Chatter

MEDIUM SEVERITY

There are no Medium Severity Issues for Hacker Chatter

LOW SEVERITY

There are no Low Severity Issues for Hacker Chatter

POSITIVE

There are no Positive Signals for Hacker Chatter

INFORMATIONAL

There are no Informational Signals for Hacker Chatter

No issues found

B 84 IP REPUTATION

The IP Reputation and Malware Exposure module makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds, and third party threat intelligence data sharing partnerships. The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures globally from all over the world. The incoming data is processed and attributed to corporate enterprises. The quantity and duration of malware infections are used as the determining factor for calculating is module the Malware Exposure Key Threat Indicator.

HIGH SEVERITY

Malware Infection	2

MEDIUM SEVERITY

There are no Medium Severity Issues for IP Reputation

LOW SEVERITY

There are no Low Severity Issues for IP Reputation

POSITIVE

There are no Positive Signals for IP Reputation

INFORMATIONAL

Malware Infection Trail	66
Potentially Vulnerable Application Installation (PVA) Trail	132
Potentially Vulnerable Application (PVA) Installation	64
Adware Installation Trail	7

Malware Infection Trail

Communications indicative of malware infections were observed over the last 365 days.

Description
After a device has been infected by malware, it often communicates with a command and control (C&C) service on the internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.
Events in this unscored issue overlap with those in the Malware Infection issue, providing visibility into the last year of malware infections.

Recommendation
Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

66 findings

MALWARE FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
conficker	sinkhole	2.192.7.145	21	3/5/2022, 6:19:45 AM
conficker	sinkhole	2.192.6.142	8	3/2/2022, 2:20:41 PM
conficker	sinkhole	2.192.0.173	4	1/28/2022, 6:37:51 AM
conficker	sinkhole	2.192.1.150	30	1/22/2022, 9:06:46 AM
conficker	sinkhole	2.192.7.62	7	1/21/2022, 12:03:53 PM
conficker	sinkhole	2.192.11.62	1	1/21/2022, 5:55:23 AM
conficker	sinkhole	2.192.4.232	1	1/21/2022, 2:51:10 AM
conficker	sinkhole	2.192.1.2	1	1/20/2022, 8:16:12 AM
conficker	sinkhole	2.192.8.132	86	10/22/2021, 5:37:10 AM
android.digitime.fota	sinkhole	2.192.11.115	2	6/16/2021, 6:19:15 PM
android.digitime.fota	sinkhole	2.192.0.53	2	6/14/2021, 6:18:07 PM
android.digitime.fota	sinkhole	2.192.7.100	2	6/13/2021, 6:59:38 PM
android.digitime.fota	sinkhole	2.192.8.188	2	6/11/2021, 6:11:49 PM
android.digitime.fota	sinkhole	2.192.4.11	2	6/8/2021, 7:20:58 PM
android.digitime.fota	sinkhole	2.192.8.219	2	6/7/2021, 6:57:20 PM
android.digitime.fota	sinkhole	2.192.9.0	2	6/6/2021, 6:03:18 PM

MALWARE FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
android.digitime.fota	sinkhole	2.192.4.146	2	6/3/2021, 6:07:56 PM
android.digitime.fota	sinkhole	2.192.6.124	2	6/1/2021, 6:52:11 PM
android.digitime.fota	sinkhole	2.192.5.202	2	5/31/2021, 6:05:48 PM
android.digitime.fota	sinkhole	2.192.10.0	2	5/29/2021, 6:33:31 PM
conficker	sinkhole	2.192.9.118	17	5/22/2021, 8:41:13 AM
mirai	darknet	2.192.2.221	1	5/16/2021, 11:46:21 AM
mirai	darknet	2.192.4.6	1	5/15/2021, 6:48:35 PM
conficker	sinkhole, unknown	2.192.7.162	13	5/14/2021, 12:53:40 PM
stealrat	unknown	2.192.5.17	6	5/11/2021, 1:55:59 AM
mirai	darknet	2.192.6.218	1	5/9/2021, 8:32:12 AM
mirai	darknet	2.192.4.37	1	5/7/2021, 10:28:21 AM
mirai	darknet	2.192.7.48	3	5/1/2021, 12:00:05 AM
mirai	darknet	2.192.7.1	1	4/30/2021, 4:32:20 PM
mirai	darknet	2.192.8.72	1	4/23/2021, 9:43:35 AM
mirai	darknet	2.192.3.163	1	4/22/2021, 6:10:28 PM
mirai	darknet	2.192.3.60	1	4/22/2021, 3:34:55 PM
mirai	darknet	2.192.11.35	1	4/22/2021, 2:25:09 PM
android.digitime.fota	sinkhole	2.192.1.119	14	4/21/2021, 11:02:27 AM
ranbyus	unknown	2.192.0.36	1	4/20/2021, 9:11:23 AM
android.digitime.fota	sinkhole	2.192.5.40	10	4/19/2021, 3:37:56 PM
tinba	unknown	2.192.0.36	1	4/18/2021, 7:34:38 PM
nymaim	unknown	2.192.0.36	1	4/18/2021, 10:09:02 AM
tinba	unknown	2.192.6.14	1	4/18/2021, 8:01:59 AM
android.digitime.fota	sinkhole	2.192.6.120	6	4/17/2021, 10:30:08 PM
android.digitime.fota	sinkhole	2.192.4.101	2	4/17/2021, 7:02:38 PM
android.digitime.fota	sinkhole	2.192.7.223	2	4/15/2021, 3:49:30 AM
android.digitime.fota	sinkhole	2.192.8.24	18	4/14/2021, 7:45:43 PM
stealrat	unknown	2.192.6.156	3	4/13/2021, 1:59:48 AM
android.digitime.fota	sinkhole	2.192.9.108	6	4/11/2021, 5:51:29 PM
mirai	darknet	2.192.5.219	1	4/7/2021, 4:57:59 PM
mirai	darknet	2.192.0.112	1	4/5/2021, 12:33:24 PM
stealrat	unknown	2.192.1.69	1	4/3/2021, 8:34:24 PM
mirai	darknet	2.192.5.153	1	4/3/2021, 9:34:33 AM
android.digitime.fota	sinkhole	2.192.6.14	2	4/2/2021, 2:41:05 AM
android.digitime.fota	sinkhole	2.192.4.149	12	4/1/2021, 6:13:19 PM
android.digitime.fota	sinkhole	2.192.5.222	2	3/31/2021, 6:54:21 PM
android.digitime.fota	sinkhole	2.192.8.251	4	3/30/2021, 5:01:22 PM
mirai	darknet	2.192.5.242	1	3/30/2021, 1:14:32 PM
android.digitime.fota	sinkhole	2.192.0.76	2	3/30/2021, 12:30:06 AM
android.digitime.fota	sinkhole	2.192.8.99	2	3/29/2021, 4:16:36 PM
android.digitime.fota	sinkhole	2.192.2.232	4	3/29/2021, 7:42:31 AM
android.digitime.fota	sinkhole	2.192.7.68	2	3/28/2021, 3:10:53 PM
stealrat	unknown	2.192.6.84	1	3/28/2021, 8:24:28 AM
mirai	darknet	2.192.7.161	1	3/26/2021, 9:31:36 AM
iotmirai	probe	2.192.7.161	1	3/26/2021, 9:31:36 AM
gamut	unknown	2.192.15.55	1	3/25/2021, 4:42:25 PM
gamut	unknown	2.192.4.42	1	3/25/2021, 12:22:12 AM
mirai	darknet	2.192.4.81	1	3/24/2021, 7:57:10 AM
iotmirai	probe	2.192.5.176	1	3/23/2021, 3:24:21 PM
mirai	darknet	2.192.5.176	1	3/23/2021, 3:24:21 PM

Potentially Vulnerable Application Installation (PVA) Trail

We detected evidence of PVA installations within the past 365 days.

Description

Potentially vulnerable applications (PVAs) have legitimate business purposes, but can pose security risks. They typically use expired domain names for communication with back-end infrastructure, so an attacker can register an expired domain and interact with a PVA. Depending on how the PVA uses the expired domain, the attacker might be able to gather information about a user and the device running the application, send commands to the application, or exploit the application to infect the device. The PVA category also covers legitimate applications that could be used by crypto mining malware; cause malware infections, as with torrent applications; cause various other security issues. This unscored

Recommendation

Investigate the devices associated with the IP addresses listed, checking for evidence of PVA installations. Watch for potentially malicious interactions between expired domains and PVAs.

issue has a longer detection period (365 days) than PVA Installation Observed (14 days), but is otherwise identical. Events within the two issue types may overlap.

132 findings

PVA FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	COMMUNICATIONS LAST OBSERVED
pva.torrent.openinternet	sinkhole	2.192.7.52	10	3/13/2022, 11:06:13 PM
pva.torrent.openinternet	sinkhole	2.192.7.216	3	3/13/2022, 11:00:14 AM
pva.torrent.openinternet	sinkhole	2.192.0.203	30	3/13/2022, 8:59:14 AM
pva.torrent.openinternet	sinkhole	2.192.13.137	7	3/9/2022, 8:26:17 PM
pva.torrent.openinternet	sinkhole	2.192.1.133	10	3/9/2022, 6:43:17 PM
pva.torrent.openinternet	sinkhole	2.192.5.221	40	3/9/2022, 6:51:31 AM
pva.torrent.openinternet	sinkhole	2.192.4.225	24	3/6/2022, 9:36:13 PM
pva.torrent.openinternet	sinkhole	2.192.8.211	10	3/5/2022, 11:58:55 PM
pva.torrent.openinternet	sinkhole	2.192.6.34	4	3/5/2022, 3:49:11 AM
pva.torrent.openinternet	sinkhole	2.192.5.226	14	3/5/2022, 1:48:11 AM
pva.torrent.openinternet	sinkhole	2.192.7.34	5	3/4/2022, 4:55:49 AM
pva.torrent.openinternet	sinkhole	2.192.8.222	23	3/4/2022, 1:53:34 AM
pva.torrent.openinternet	sinkhole	2.192.10.69	18	3/2/2022, 9:42:01 PM
pva.torrent.openinternet	sinkhole	2.192.3.43	4	3/2/2022, 4:52:16 AM
pva.torrent.openinternet	sinkhole	2.192.1.144	6	3/2/2022, 2:51:16 AM
pva.torrent.openinternet	sinkhole	2.192.7.227	10	3/1/2022, 11:50:16 PM
pva.torrent.openinternet	sinkhole	2.192.2.136	6	3/1/2022, 2:23:14 PM
pva.torrent.openinternet	sinkhole	2.192.3.223	2	3/1/2022, 12:39:30 PM
pva.torrent.openinternet	sinkhole	2.192.5.169	4	3/1/2022, 6:32:59 AM
pva.torrent.openinternet	sinkhole	2.192.5.50	4	3/1/2022, 5:40:32 AM
pva.torrent.openinternet	sinkhole	2.192.7.131	3	3/1/2022, 2:39:48 AM
pva.torrent.openinternet	sinkhole	2.192.6.189	12	3/1/2022, 12:38:48 AM
pva.torrent.openinternet	sinkhole	2.192.5.106	10	2/28/2022, 8:31:20 PM
pva.torrent.openinternet	sinkhole	2.192.5.31	10	2/28/2022, 2:33:48 PM
pva.torrent.openinternet	sinkhole	2.192.9.24	5	2/28/2022, 5:29:57 AM
pva.torrent.openinternet	sinkhole	2.192.1.21	14	2/28/2022, 2:27:42 AM
pva.torrent.openinternet	sinkhole	2.192.6.157	10	2/27/2022, 8:45:41 PM
pva.torrent.openinternet	sinkhole	2.192.1.165	56	2/27/2022, 3:38:26 AM
pva.torrent.openinternet	sinkhole	2.192.5.48	15	2/26/2022, 10:21:07 PM
pva.torrent.openinternet	sinkhole	2.192.8.248	9	2/25/2022, 4:35:53 PM
pva.torrent.openinternet	sinkhole	2.192.4.42	19	2/24/2022, 5:43:43 PM
pva.torrent.openinternet	sinkhole	2.192.4.142	4	2/22/2022, 3:01:33 AM
pva.torrent.openinternet	sinkhole	2.192.0.29	6	2/22/2022, 12:00:48 AM
pva.torrent.openinternet	sinkhole	2.192.5.115	7	2/21/2022, 7:58:48 PM
pva.torrent.openinternet	sinkhole	2.192.4.203	40	2/21/2022, 4:52:42 PM
pva.torrent.openinternet	sinkhole	2.192.1.53	10	2/18/2022, 10:21:48 PM
pva.torrent.kickasstracker	sinkhole	2.192.11.230	2	2/18/2022, 8:43:31 PM
pva.torrent.openinternet	sinkhole	2.192.11.230	2	2/18/2022, 8:43:29 PM
pva.torrent.openinternet	sinkhole	2.192.0.25	5	2/18/2022, 3:11:36 AM
pva.torrent.openinternet	sinkhole	2.192.1.131	1	2/18/2022, 12:09:21 AM
pva.torrent.openinternet	sinkhole	2.192.3.34	10	2/17/2022, 11:09:36 PM
pva.torrent.openinternet	sinkhole	2.192.6.221	14	2/17/2022, 12:34:32 PM
pva.torrent.openinternet	sinkhole	2.192.11.91	1	2/17/2022, 11:39:10 AM
pva.torrent.openinternet	sinkhole	2.192.5.179	10	2/17/2022, 10:39:25 AM
pva.torrent.openinternet	sinkhole	2.192.8.3	20	2/17/2022, 3:20:46 AM
pva.torrent.openinternet	sinkhole	2.192.9.9	16	2/16/2022, 4:10:53 PM
pva.torrent.openinternet	sinkhole	2.192.10.199	8	2/16/2022, 1:07:56 PM
pva.torrent.openinternet	sinkhole	2.192.1.140	22	2/16/2022, 11:06:49 AM
pva.torrent.openinternet	sinkhole	2.192.9.87	10	2/16/2022, 8:04:08 AM
pva.torrent.openinternet	sinkhole	2.192.1.135	6	2/16/2022, 3:48:41 AM
pva.torrent.openinternet	sinkhole	2.192.5.160	12	2/16/2022, 2:37:41 AM
pva.torrent.openinternet	sinkhole	2.192.0.105	10	2/15/2022, 11:35:44 PM
pva.torrent.openinternet	sinkhole	2.192.7.23	10	2/15/2022, 9:54:55 PM
pva.torrent.openinternet	sinkhole	2.192.5.240	10	2/15/2022, 8:42:38 PM
pva.torrent.openinternet	sinkhole	2.192.6.49	10	2/15/2022, 6:40:50 PM
pva.torrent.openinternet	sinkhole	2.192.10.187	10	2/15/2022, 4:24:35 AM
pva.torrent.openinternet	sinkhole	2.192.9.200	10	2/15/2022, 2:17:45 AM
pva.torrent.openinternet	sinkhole	2.192.9.19	10	2/14/2022, 11:22:40 PM
pva.torrent.openinternet	sinkhole	2.192.5.77	6	2/14/2022, 5:14:54 AM
pva.torrent.openinternet	sinkhole	2.192.4.85	3	2/14/2022, 2:14:06 AM
pva.torrent.openinternet	sinkhole	2.192.0.46	12	2/14/2022, 12:13:14 AM
pva.torrent.openinternet	sinkhole	2.192.2.62	6	2/13/2022, 3:04:09 AM
pva.torrent.openinternet	sinkhole	2.192.4.155	11	2/13/2022, 12:02:06 AM
pva.torrent.openinternet	sinkhole	2.192.7.51	2	2/12/2022, 2:29:07 AM
pva.torrent.openinternet	sinkhole	2.192.0.211	8	2/11/2022, 9:41:07 PM

PVA FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	COMMUNICATIONS LAST OBSERVED
pva.torrent.openinternet	sinkhole	2.192.2.194	15	2/8/2022, 7:35:31 AM
pva.torrent.openinternet	sinkhole	2.192.1.252	24	2/4/2022, 5:36:58 PM
pva.torrent.openinternet	sinkhole	2.192.3.51	9	2/4/2022, 12:04:13 AM
pva.torrent.openinternet	sinkhole	2.192.4.31	7	2/3/2022, 2:31:29 PM
pva.torrent.openinternet	sinkhole	2.192.7.108	5	2/1/2022, 9:43:25 PM
pva.torrent.openinternet	sinkhole	2.192.1.38	18	1/30/2022, 2:26:08 PM
pva.torrent.openinternet	sinkhole	2.192.1.179	14	1/29/2022, 1:16:13 AM
pva.torrent.openinternet	sinkhole	2.192.8.170	10	1/28/2022, 10:30:50 PM
pva.torrent.openinternet	sinkhole	2.192.0.42	3	1/28/2022, 9:58:45 PM
pva.torrent.openinternet	sinkhole	2.192.11.93	2	1/28/2022, 4:35:47 PM
pva.torrent.openinternet	sinkhole	2.192.6.66	7	1/26/2022, 5:22:14 PM
pva.torrent.openinternet	sinkhole	2.192.10.183	1	1/24/2022, 9:40:00 AM
pva.torrent.openinternet	sinkhole	2.192.0.79	5	1/24/2022, 8:57:58 AM
pva.torrent.kickasstracker	sinkhole	2.192.1.112	6	1/18/2022, 11:37:23 PM
pva.torrent.openinternet	sinkhole	2.192.1.112	3	1/18/2022, 10:50:54 PM
pva.torrent.openinternet	sinkhole	2.192.2.105	1	1/16/2022, 8:13:14 AM
pva.torrent.openinternet	sinkhole	2.192.11.23	3	1/16/2022, 1:32:51 AM
pva.torrent.openinternet	sinkhole	2.192.4.228	4	1/15/2022, 11:54:06 PM
pva.torrent.openinternet	sinkhole	2.192.1.77	6	1/15/2022, 11:18:01 PM
pva.torrent.openinternet	sinkhole	2.192.10.174	10	1/15/2022, 10:53:16 PM
pva.torrent.openinternet	sinkhole	2.192.8.86	13	1/15/2022, 7:49:53 PM
pva.torrent.openinternet	sinkhole	2.192.9.144	10	1/13/2022, 10:09:15 AM
pva.torrent.openinternet	sinkhole	2.192.5.249	1	1/12/2022, 6:19:22 PM
pva.torrent.openinternet	sinkhole	2.192.3.136	10	1/12/2022, 5:55:32 PM
pva.torrent.openinternet	sinkhole	2.192.6.191	27	1/11/2022, 8:07:42 PM
pva.torrent.kickasstracker	sinkhole	2.192.6.191	1	1/9/2022, 11:11:45 AM
pva.torrent.openinternet	sinkhole	2.192.7.37	20	1/9/2022, 10:26:09 AM
pva.torrent.kickasstracker	sinkhole	2.192.7.37	10	1/8/2022, 11:44:09 PM
pva.torrent.openinternet	sinkhole	2.192.6.137	10	1/2/2022, 1:42:12 PM
pva.torrent.kickasstracker	sinkhole	2.192.2.197	1	12/30/2021, 9:09:31 AM
pva.torrent.openinternet	sinkhole	2.192.6.54	10	12/29/2021, 4:39:35 PM
pva.torrent.openinternet	sinkhole	2.192.4.242	20	12/23/2021, 11:01:55 PM
pva.torrent.openinternet	sinkhole	2.192.32.88	56	12/22/2021, 4:44:22 PM
pva.soundink	sinkhole	2.192.6.245	14	12/17/2021, 3:23:03 PM
pva.torrent.openinternet	sinkhole	2.192.7.86	1	12/12/2021, 10:27:52 AM
pva.torrent.openinternet	sinkhole	2.192.7.135	2	12/11/2021, 4:50:50 PM
pva.torrent.openinternet	sinkhole	2.192.4.92	10	12/9/2021, 8:28:14 PM
pva.torrent.openinternet	sinkhole	2.192.5.128	10	12/9/2021, 11:12:32 AM
pva.torrent.openinternet	sinkhole	2.192.0.210	15	12/9/2021, 1:23:31 AM
pva.torrent.kickasstracker	sinkhole	2.192.5.38	1	12/7/2021, 7:28:12 AM
pva.torrent.kickasstracker	sinkhole	2.192.4.146	3	12/7/2021, 1:41:00 AM
pva.torrent.kickasstracker	sinkhole	2.192.3.247	1	12/7/2021, 12:06:51 AM
pva.torrent.kickasstracker	sinkhole	2.192.4.0	4	12/6/2021, 11:35:28 PM
pva.torrent.kickasstracker	sinkhole	2.192.2.181	5	12/6/2021, 9:29:56 PM
pva.torrent.kickasstracker	sinkhole	2.192.5.215	1	12/6/2021, 6:53:01 PM
pva.torrent.kickasstracker	sinkhole	2.192.5.14	3	12/6/2021, 6:21:38 PM
pva.torrent.kickasstracker	sinkhole	2.192.9.29	1	12/6/2021, 4:47:29 PM
pva.torrent.kickasstracker	sinkhole	2.192.6.255	9	12/6/2021, 4:16:06 PM
pva.torrent.openinternet	sinkhole	2.192.4.210	10	12/2/2021, 9:35:22 PM
pva.torrent.openinternet	sinkhole	2.192.10.6	10	11/27/2021, 7:57:28 PM
pva.torrent.openinternet	sinkhole	2.192.1.123	3	11/27/2021, 7:52:47 AM
pva.torrent.openinternet	sinkhole	2.192.5.5	5	11/27/2021, 5:51:55 AM
pva.torrent.openinternet	sinkhole	2.192.6.252	46	11/27/2021, 2:50:37 AM
pva.torrent.openinternet	sinkhole	2.192.32.69	6	11/26/2021, 6:37:42 AM
pva.torrent.openinternet	sinkhole	2.192.1.33	5	11/23/2021, 7:51:22 AM
pva.torrent.openinternet	sinkhole	2.192.5.232	6	11/23/2021, 5:07:20 AM
pva.torrent.openinternet	sinkhole	2.192.0.144	9	11/23/2021, 2:05:32 AM
pva.torrent.openinternet	sinkhole	2.192.0.89	3	11/22/2021, 11:15:32 PM
pva.torrent.openinternet	sinkhole	2.192.1.12	2	11/22/2021, 9:10:40 PM
pva.torrent.openinternet	sinkhole	2.192.4.234	2	11/18/2021, 9:54:42 PM
pva.torrent.openinternet	sinkhole	2.192.5.37	10	11/18/2021, 9:20:07 PM
pva.torrent.openinternet	sinkhole	2.192.32.131	7	11/18/2021, 9:19:24 PM
pva.torrent.openinternet	sinkhole	2.192.9.62	3	11/15/2021, 5:23:45 PM
pva.torrent.openinternet	sinkhole	2.192.7.77	10	11/11/2021, 5:42:49 PM
pva.torrent.openinternet	sinkhole	2.192.0.83	25	11/11/2021, 3:28:32 AM
pva.torrent.openinternet	sinkhole	2.192.7.11	3	10/10/2021, 1:10:45 PM
pva.torrent.openinternet	sinkhole	2.192.32.123	10	9/1/2021, 9:43:01 PM

Potentially Vulnerable Application (PVA) Installation

We detected evidence of PVA installations within the past 30 days.

Description
Potentially vulnerable applications (PVAs) have legitimate business purposes, but can pose security risks. They typically use expired domain names for communication with back-end infrastructure, so an attacker can register an expired domain and interact with a PVA. Depending on how the PVA uses the expired domain, the attacker might be able to gather information about a user and the device running the application, send commands to the application, or exploit the application to infect the device. The PVA category also covers legitimate applications that could be used by crypto mining malware; cause malware infections, as with torrent applications; cause various other security issues.

Recommendation
Investigate the devices associated with the IP addresses listed, checking for evidence of PVA installations. Watch for potentially malicious interactions between expired domains and PVAs.

64 findings

PVA FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	COMMUNICATIONS LAST OBSERVED
pva.torrent.openinternet	sinkhole	2.192.7.52	10	3/13/2022, 11:06:13 PM
pva.torrent.openinternet	sinkhole	2.192.7.216	3	3/13/2022, 11:00:14 AM
pva.torrent.openinternet	sinkhole	2.192.0.203	30	3/13/2022, 8:59:14 AM
pva.torrent.openinternet	sinkhole	2.192.13.137	7	3/9/2022, 8:26:17 PM
pva.torrent.openinternet	sinkhole	2.192.1.133	10	3/9/2022, 6:43:17 PM
pva.torrent.openinternet	sinkhole	2.192.5.221	40	3/9/2022, 6:51:31 AM
pva.torrent.openinternet	sinkhole	2.192.4.225	24	3/6/2022, 9:36:13 PM
pva.torrent.openinternet	sinkhole	2.192.8.211	10	3/5/2022, 11:58:55 PM
pva.torrent.openinternet	sinkhole	2.192.6.34	4	3/5/2022, 3:49:11 AM
pva.torrent.openinternet	sinkhole	2.192.5.226	14	3/5/2022, 1:48:11 AM
pva.torrent.openinternet	sinkhole	2.192.7.34	5	3/4/2022, 4:55:49 AM
pva.torrent.openinternet	sinkhole	2.192.8.222	23	3/4/2022, 1:53:34 AM
pva.torrent.openinternet	sinkhole	2.192.10.69	18	3/2/2022, 9:42:01 PM
pva.torrent.openinternet	sinkhole	2.192.3.43	4	3/2/2022, 4:52:16 AM
pva.torrent.openinternet	sinkhole	2.192.1.144	6	3/2/2022, 2:51:16 AM
pva.torrent.openinternet	sinkhole	2.192.7.227	10	3/1/2022, 11:50:16 PM
pva.torrent.openinternet	sinkhole	2.192.2.136	2	3/1/2022, 2:23:14 PM
pva.torrent.openinternet	sinkhole	2.192.3.223	2	3/1/2022, 12:39:30 PM
pva.torrent.openinternet	sinkhole	2.192.5.169	4	3/1/2022, 6:32:59 AM
pva.torrent.openinternet	sinkhole	2.192.5.50	4	3/1/2022, 5:40:32 AM
pva.torrent.openinternet	sinkhole	2.192.7.131	3	3/1/2022, 2:39:48 AM
pva.torrent.openinternet	sinkhole	2.192.6.189	12	3/1/2022, 12:38:48 AM
pva.torrent.openinternet	sinkhole	2.192.5.106	10	2/28/2022, 8:31:20 PM
pva.torrent.openinternet	sinkhole	2.192.5.31	10	2/28/2022, 2:33:48 PM
pva.torrent.openinternet	sinkhole	2.192.9.24	5	2/28/2022, 5:29:57 AM
pva.torrent.openinternet	sinkhole	2.192.1.21	14	2/28/2022, 2:27:42 AM
pva.torrent.openinternet	sinkhole	2.192.6.157	10	2/27/2022, 8:45:41 PM
pva.torrent.openinternet	sinkhole	2.192.1.165	56	2/27/2022, 3:38:26 AM
pva.torrent.openinternet	sinkhole	2.192.5.48	15	2/26/2022, 10:21:07 PM
pva.torrent.openinternet	sinkhole	2.192.8.248	9	2/25/2022, 4:35:53 PM
pva.torrent.openinternet	sinkhole	2.192.4.42	19	2/24/2022, 5:43:43 PM
pva.torrent.openinternet	sinkhole	2.192.4.142	4	2/22/2022, 3:01:33 AM
pva.torrent.openinternet	sinkhole	2.192.0.29	6	2/22/2022, 12:00:48 AM
pva.torrent.openinternet	sinkhole	2.192.5.115	7	2/21/2022, 7:58:48 PM
pva.torrent.openinternet	sinkhole	2.192.4.203	40	2/21/2022, 4:52:42 PM
pva.torrent.openinternet	sinkhole	2.192.1.53	10	2/18/2022, 10:21:48 PM
pva.torrent.kickasstracker	sinkhole	2.192.11.230	2	2/18/2022, 8:43:31 PM
pva.torrent.openinternet	sinkhole	2.192.11.230	2	2/18/2022, 8:43:29 PM
pva.torrent.openinternet	sinkhole	2.192.0.25	5	2/18/2022, 3:11:36 AM
pva.torrent.openinternet	sinkhole	2.192.1.131	1	2/18/2022, 12:09:21 AM
pva.torrent.openinternet	sinkhole	2.192.3.34	10	2/17/2022, 11:09:36 PM
pva.torrent.openinternet	sinkhole	2.192.6.221	14	2/17/2022, 12:34:32 PM
pva.torrent.openinternet	sinkhole	2.192.11.91	1	2/17/2022, 11:39:10 AM
pva.torrent.openinternet	sinkhole	2.192.5.179	10	2/17/2022, 10:39:25 AM
pva.torrent.openinternet	sinkhole	2.192.8.3	20	2/17/2022, 3:20:46 AM
pva.torrent.openinternet	sinkhole	2.192.9.9	10	2/16/2022, 4:10:53 PM
pva.torrent.openinternet	sinkhole	2.192.10.199	8	2/16/2022, 1:07:56 PM
pva.torrent.openinternet	sinkhole	2.192.1.140	22	2/16/2022, 11:06:49 AM
pva.torrent.openinternet	sinkhole	2.192.9.87	10	2/16/2022, 8:04:08 AM
pva.torrent.openinternet	sinkhole	2.192.1.135	6	2/16/2022, 3:48:41 AM
pva.torrent.openinternet	sinkhole	2.192.5.160	12	2/16/2022, 2:37:41 AM
pva.torrent.openinternet	sinkhole	2.192.0.105	10	2/15/2022, 11:35:44 PM

PVA FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	COMMUNICATIONS LAST OBSERVED
pva.torrent.openinternet	sinkhole	2.192.7.23	10	2/15/2022, 9:54:55 PM
pva.torrent.openinternet	sinkhole	2.192.5.240	10	2/15/2022, 8:42:38 PM
pva.torrent.openinternet	sinkhole	2.192.6.49	10	2/15/2022, 6:40:50 PM
pva.torrent.openinternet	sinkhole	2.192.10.187	10	2/15/2022, 4:24:35 AM
pva.torrent.openinternet	sinkhole	2.192.9.200	10	2/15/2022, 2:17:45 AM
pva.torrent.openinternet	sinkhole	2.192.9.19	10	2/14/2022, 11:22:40 PM
pva.torrent.openinternet	sinkhole	2.192.5.77	6	2/14/2022, 5:14:54 AM
pva.torrent.openinternet	sinkhole	2.192.4.85	3	2/14/2022, 2:14:06 AM
pva.torrent.openinternet	sinkhole	2.192.0.46	12	2/14/2022, 12:13:14 AM
pva.torrent.openinternet	sinkhole	2.192.2.62	6	2/13/2022, 3:04:09 AM
pva.torrent.openinternet	sinkhole	2.192.4.155	11	2/13/2022, 12:02:06 AM
pva.torrent.openinternet	sinkhole	2.192.7.51	2	2/12/2022, 2:29:07 AM

Adware Installation Trail

Communications indicative of adware installations were observed over the last 365 days.

Description
After adware has been installed on a device, it often communicates with a service on the Internet. This service allows the adware to register the device on which it is installed and receive the advertisements that will be displayed to the user.
Events in this unscored issue overlap with those in the Adware Installation issue, providing visibility into the last year of adware installations.

Recommendation
Investigate the devices associated with the IP addresses listed, checking for evidence of adware installations.

7 findings

ADWARE FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
pua.android.cheetah	sinkhole	2.192.2.118	1	2/11/2022, 7:00:52 AM
pua.android.cheetah	sinkhole	2.192.4.176	2	2/1/2022, 5:35:35 PM
pua.android.cheetah	sinkhole	2.192.3.141	1	1/8/2022, 9:49:18 PM
adware.grambler	sinkhole	2.192.2.50	10	12/13/2021, 6:51:47 PM
pua.android.cheetah	sinkhole	2.192.5.88	1	11/28/2021, 1:18:37 PM
pua.android.cheetah	sinkhole	2.192.12.245	1	11/19/2021, 5:42:04 PM
pua.android.cheetah	sinkhole	2.192.1.92	27	10/11/2021, 11:23:47 AM

Malware Infection

-1.0 SCORE IMPACT

Communications indicative of malware infections were observed over the last 30 days.

Description
After a device has been infected by malware, it often communicates with a command and control (C&C) service on the Internet. This service allows the malware to register its infected device and receive instructions from the malware's authors. These instructions could cause the device to delete or encrypt its datastores, participate in distributed denial-of-service (DDoS) attacks, or perform any variety of malicious actions.

Recommendation
Investigate the devices associated with the IP addresses listed, checking for evidence of malware infections.

2 findings

MALWARE FAMILY	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
conficker	sinkhole	2.192.7.145	21	3/5/2022, 6:19:45 AM
conficker	sinkhole	2.192.6.142	8	3/2/2022, 2:20:41 PM

A 100 INFORMATION LEAK

This Information Leak module makes use of chatter monitoring and deep web monitoring capabilities to identify compromised credentials being circulated by hackers. These come in the form of bulk data breaches announced publicly as well as smaller breaches, and smaller exchanges between hackers

HIGH SEVERITY

There are no High Severity Issues for Information Leak

MEDIUM SEVERITY

There are no Medium Severity Issues for Information Leak

LOW SEVERITY

There are no Low Severity Issues for Information Leak

POSITIVE

There are no Positive Signals for Information Leak

INFORMATIONAL

There are no Informational Signals for Information Leak

No issues found

F 51 NETWORK SECURITY

The Network Security module checks public datasets for evidence of high risk or insecure open ports within the company network. Insecure ports can often be exploited to allow an attacker to circumvent the login process or obtain elevated access to the system. If misconfigured, the open port can act as the entry point between a hacker's workstation and your internal network

HIGH SEVERITY

Industrial Control System Device Accessible	3
SSL/TLS Service Supports Weak Protocol	17
SSH Software Supports Vulnerable Protocol	1

MEDIUM SEVERITY

Certificate Is Self-Signed	161
Remote Access Service Observed	1
TLS Service Supports Weak Cipher Suite	61
Certificate Signed With Weak Algorithm	59
SSH Supports Weak MAC	1
RDP Service Observed	1
Certificate Is Expired	64
PPTP Service Accessible	1
SSH Supports Weak Cipher	1

LOW SEVERITY

Certificate Without Revocation Control	194
FTP Service Observed	30
Certificate Lifetime Is Longer Than Best Practices	111
Telnet Service Observed	34
IP Camera Accessible	8

POSITIVE

There are no Positive Signals for Network Security

INFORMATIONAL

HTTP Proxy Service Detected	3
Embedded IOT Web Server Exposed	1
Networking Service Observed	3
DNS Server Accessible	2
UPnP Accessible	2

Certificate Is Self-Signed

-1.4 SCORE IMPACT

Self-signed certificates prevent TLS clients from connecting to servers.

Description

When a certificate is issued, it is signed by a private key. Publicly-accessible services should have certificates signed by keys associated with certificate authorities (CA). The credentials of certificate authorities are stored in a table called the trust store which is baked into modern web browsers and operating systems. Certificates signed by keys not in the trust store prevent TLS clients from connecting to servers.
Off-the-shelf software and hardware frequently runs services that use self-signed certificates by default. If these services are publicly-accessible then they should be configured to use certificates issued by known certificate authorities. Failure to do so exposes users of the service to man-in-the-middle attacks on the open Internet.
Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

Recommendation

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

161 findings

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.0.111	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/11/2022, 2:00:46 PM
2.192.1.99	495e762b5aa7fd9dd83c3947f94f0d91f0f1d0a2722b346f07f2038ea4525f5f3	1	3/11/2022, 7:20:14 AM
2.192.1.171	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/11/2022, 7:16:49 AM
2.192.1.62	66c0195145de59bff811f7ccb3f9487a15f2a105dd98347ccfeb939c8521c5e6e	1	3/11/2022, 7:12:56 AM
2.192.1.149	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/11/2022, 7:03:49 AM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.1.106	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 7:03:20 AM
2.192.1.60	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	3/11/2022, 6:55:28 AM
2.192.7.192	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 1:31:43 AM
2.192.2.167	ac3395fbaecd3bc28bd6420dc5d99a3eef1789819b45bdc0d60abe410a63559c9	1	3/10/2022, 7:43:19 PM
2.192.2.159	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/10/2022, 7:36:06 PM
2.192.0.92	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 7:33:33 PM
2.192.0.56	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 7:27:22 PM
2.192.8.177	72403d4f01fccf8e13e830a61bb64004de1a58034b5be80947f6b81177a03b45	1	3/10/2022, 6:41:15 PM
2.192.8.23	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 6:37:48 PM
2.192.8.234	57ef50936a84664f41134c375c372c61917e1a9480436eeb19eb8ea074b43503	1	3/10/2022, 6:34:54 PM
2.192.3.195	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 4:41:11 PM
2.192.3.58	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/10/2022, 4:37:17 PM
2.192.3.112	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 3:56:39 PM
2.192.1.141	bb826cd36f3b6f01458e391802a7068b3716f4c214de14760c95670f951abe53	1	3/10/2022, 11:37:01 AM
2.192.11.136	983033524ba5518ed3f22df894c80b06d14d792dffe3b275495d6e9a5ce76cf9c	1	3/10/2022, 7:29:28 AM
2.192.10.86	a6951a61b0adf3e54897349d17de9f0c3701f20012eee9a7170b1aaddf8e89b79	1	3/10/2022, 7:25:56 AM
2.192.11.62	ee5e83ea61be05e0b8ef9782344d809abd1aabad10ac1019bf3aeaaa9a98d9af	1	3/10/2022, 7:25:29 AM
2.192.11.209	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 7:20:47 AM
2.192.11.106	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	3/10/2022, 7:15:35 AM
2.192.11.21	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 7:14:51 AM
2.192.7.68	3d42db219fb46a96b8223836774b054f5514a5f5daded827e5c63bb5641793f4c	1	3/10/2022, 6:54:51 AM
2.192.7.247	bd503c3b956fd2f76fd80b8e11100909b064dcb30f629e3e6b06c997416b862b	1	3/10/2022, 6:47:41 AM
2.192.7.62	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 6:37:23 AM
2.192.10.171	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 6:34:21 AM
2.192.10.53	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 6:31:04 AM
2.192.11.229	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	3/10/2022, 6:26:17 AM
2.192.10.65	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc03264661f80d687484	1	3/10/2022, 6:17:09 AM
2.192.11.111	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 6:15:47 AM
2.192.6.165	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 4:38:09 AM
2.192.5.79	2b88cd6a6862e630db53858fd905a1911fc8ba1139ceddc11cce0bc7394c2e83	1	3/10/2022, 4:20:25 AM
2.192.5.239	ef1fd069e6f4fa81e139cb39d0bb049cca48e49808a04193e4674667089d1343	1	3/10/2022, 3:58:57 AM
2.192.6.13	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 3:55:12 AM
2.192.5.158	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 3:53:36 AM
2.192.5.166	1036a96b07223f3ac421e92f3f3f1221ee89198ff875c1e3448c870bbb6d881f2	1	3/10/2022, 3:46:45 AM
2.192.5.199	6be36afe45749ce202b1d2ba52e9dd30e14e2dafdf4872b391650d18fe20fd7e0	1	3/10/2022, 3:39:54 AM
2.192.2.118	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/9/2022, 9:10:26 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.2.80	f79bb73f856f690b2a8396b18ca2248002 3161636760e586149949bccff03f52	1	3/9/2022, 9:05:48 PM
2.192.2.18	8a6511e0835f5bbd71a34a273c91d5cabd3 0af2a79e3b88a103a6f61c34691d0	1	3/9/2022, 8:55:31 PM
2.192.2.171	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912	1	3/9/2022, 8:54:18 PM
2.192.2.175	a9ddd4aa8b5c6049d87b2654e2326244 4f91befda60c7a4c3d8bc8ed6aff417b	1	3/9/2022, 8:51:05 PM
2.192.4.141	49a9d29d80d87b8ecc3a7874585d07f39 53cf9d0dfd465169eaa87abcacd9dee	1	3/9/2022, 6:59:45 PM
2.192.4.253	b26beb56f515052d6a9e7db1f34d24c7b9 dba533c54adc60782dcb2682e27566	1	3/9/2022, 6:49:32 PM
2.192.1.4	bbecca6f745bc239331bd4b3cee07493d51 04ee0965a055a04f487fc9141baf6d	1	3/9/2022, 5:50:43 AM
2.192.0.236	c0a50cd4f6db9282bb7547f9787e007f691 448a3af15c37c566359496d5eb446a	1	3/9/2022, 5:49:42 AM
2.192.0.234	be8aaaad93b39f9007a5ac6fadf236616f3 d38b3dbba258b36bc2d2c80703e01	1	3/9/2022, 5:47:27 AM
2.192.0.133	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 5:46:21 AM
2.192.0.211	bbecca6f745bc239331bd4b3cee07493d51 04ee0965a055a04f487fc9141baf6d	1	3/9/2022, 5:28:35 AM
2.192.7.148	98b4742f431440761c7fd201eec206c44661 3ca0b3beee347d56f04cf792e89f4	1	3/9/2022, 4:23:34 AM
2.192.6.55	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 2:02:00 AM
2.192.6.23	c7fd6d5d51e06ba71fea12d27f8e646b1d7f ecd845c5d50f584949b0fa58dfd3	1	3/9/2022, 1:51:10 AM
2.192.6.242	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 1:48:02 AM
2.192.7.7	1d6b73c5b8c91774e7a2a993759d71ebd18 46c0fb6234f5a167e574eadd40312	1	3/9/2022, 1:43:46 AM
2.192.6.218	1e33fae1dfa19928f1d739b821ff9f14c5bc98 5fe746e20f1510a1eea3d8ed7b	1	3/9/2022, 1:37:44 AM
2.192.6.54	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912	1	3/9/2022, 1:37:35 AM
2.192.5.128	d8664eaf6fba634791ff6d3b9ae26c0d6c21 a4a5ac54868d58a243358ed12737a	1	3/9/2022, 12:55:57 AM
2.192.9.143	cc4a8a5280beac5f97de1fc9a8be98ad178 1e3f1e7887accf7ad1239ef919729	1	3/8/2022, 6:59:13 PM
2.192.9.236	15e291ef2b9d8a5316714c3a48898e9abfb 07bd90fb287d3ef2dab747183daa3	1	3/8/2022, 6:49:22 PM
2.192.9.125	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912	1	3/8/2022, 6:48:03 PM
2.192.4.34	7905ac7ab222693a18abc2bad129e1dc9191 8f5ec61faf3f82c64e3d6becaac1d	1	3/8/2022, 6:47:24 PM
2.192.9.126	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912	1	3/8/2022, 6:46:48 PM
2.192.9.199	e45500a6cb74a7dc30628d79e4ec4ba9f a7dd0fe404b270b249e766a61d6ac82	1	3/8/2022, 6:45:50 PM
2.192.4.48	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:45:11 PM
2.192.10.6	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:34:25 PM
2.192.4.41	94eaa1c54a054b484868342bd9e6d6ec5 256e4ef2ec655b2063e438d814cb191	1	3/8/2022, 6:34:21 PM
2.192.9.144	98b4742f431440761c7fd201eec206c44661 3ca0b3beee347d56f04cf792e89f4	1	3/8/2022, 6:11:38 PM
2.192.9.104	8a6511e0835f5bbd71a34a273c91d5cabd3 0af2a79e3b88a103a6f61c34691d0	1	3/8/2022, 6:11:35 PM
2.192.9.112	743f6840b846750b764eb65a556ae1e2b 83862ab59ee0e5388e06a9c0f3297f2	1	3/8/2022, 6:05:08 PM
2.192.10.132	68327011912c6be3059a32c0f97e92be82 97506cc927b1f641c74508ab7e55cc	1	3/6/2022, 1:23:47 AM
2.192.0.202	bbecca6f745bc239331bd4b3cee07493d51 04ee0965a055a04f487fc9141baf6d	1	3/6/2022, 12:19:31 AM
2.192.2.34	1036a96b07223f3ac421e92f3f3f1221ee891 98ff875c1e3448c870bbb6d881f2	1	2/16/2022, 6:19:52 AM
2.192.11.5	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 1:07:54 PM
2.192.10.229	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 1:05:41 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.4.228	4fec42fbb2a17a39e02c9a03e24d5e7a54e715b964cfb2fd8231367ea4a7fade	1	2/15/2022, 10:31:41 AM
2.192.6.143	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 10:04:50 AM
2.192.9.145	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 9:28:06 AM
2.192.9.144	13dcd3ff251061088dfe72eb3006978677359022d9a90d1a2d30655e1ad24382	1	2/15/2022, 9:28:05 AM
2.192.0.44	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 9:19:40 AM
2.192.4.109	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 6:47:55 AM
2.192.8.94	c4a148013f7b023b84b003e316626c52cbe5ea128a378beabb1a19254073ff2d	1	2/15/2022, 2:19:50 AM
2.192.10.36	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91fffbed0befd862afe1c8c	1	2/11/2022, 10:33:43 AM
2.192.5.162	7905ac7ab222693a18abc2bad129e1dc9198f5ec61faf3f82c64e3d6becaac1d	1	2/11/2022, 10:05:12 AM
2.192.5.172	6f503ea0843c3228b3704cce7c4c6f1e3e4421ed960ce8260506c959bd841e86	1	2/11/2022, 10:00:41 AM
2.192.4.237	af10a28e8fc466dc62a2aa6247ec5b1daec8b77e9cf0bb5ecf54ecc57da91fee	1	2/11/2022, 9:56:44 AM
2.192.5.58	80e089dd74979ae84d9a2e1b45c698726adafcec4c6ca183b9f3f7f0cdb2e542	1	2/11/2022, 9:55:34 AM
2.192.5.182	a9ddd4aa8b5c6049d87b2654e2326244 4f91befda60c7a4c3d8bc8ed6aff417b	1	2/11/2022, 9:51:02 AM
2.192.4.185	7f621bb6fa2ad11096c354dad397b3d6fc711737fee400c0f3a92d3bf991f6403	1	2/11/2022, 9:48:04 AM
2.192.2.174	c80b2e6bf2c33cd85bbb2220a301f3ccc0101e43355de8cff04b1274eb6f85414	1	2/11/2022, 9:39:12 AM
2.192.6.118	728a52efa109420a1c892041e9637280e43b3d7f4547435e24bab02b6cd3aff6	1	2/11/2022, 6:23:45 AM
2.192.6.243	3fea6e1fdc8aeac6463615badb58eaccc4cc2b092e27bdd1693adf1250189741	1	2/11/2022, 6:23:37 AM
2.192.11.69	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/11/2022, 12:16:45 AM
2.192.3.159	1172d82213af66fba30f80af18572648b2d38b524e238206bde88a131892ea78	1	2/10/2022, 11:09:44 PM
2.192.3.121	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	2/10/2022, 11:05:03 PM
2.192.3.75	27d8bf86ebc677f9455c823cecab4c800ac32f47abacac38962cfc04417525be	2	2/10/2022, 11:02:42 PM
2.192.3.232	8c4129a0634eba1a1d341815ef59f64b6a5c1d03ad0ede85e9f31e29545dce082	1	2/10/2022, 11:02:29 PM
2.192.3.100	85eb21e49e9d8b2797747dffde96ba01236bd9c14e6b0ae1e6c7b544c706bf44	1	2/10/2022, 11:01:28 PM
2.192.3.135	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 11:01:16 PM
2.192.3.59	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/10/2022, 10:56:12 PM
2.192.0.38	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 8:13:33 PM
2.192.0.250	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	2/10/2022, 8:03:45 PM
2.192.0.100	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/10/2022, 8:02:09 PM
2.192.0.155	00cf2c6fdad819da6310cbd9b5a53ea5c37366dcc2c529f3683203f8bcf09cca	1	2/10/2022, 8:02:02 PM
2.192.0.79	49a9d29d80d87b8ecc3a7874585d07f3953cf9d0dfd465169eaa87abcacd9dee	1	2/10/2022, 7:54:03 PM
2.192.10.64	547ff655f1ef78800409f359730bc20f737e3a566e8eabb3a0106586c100aca2	1	2/10/2022, 7:53:51 PM
2.192.10.73	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 7:47:50 PM
2.192.5.250	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 6:45:29 AM
2.192.6.3	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/10/2022, 6:39:53 AM
2.192.6.210	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91fffbed0befd862afe1c8c	1	2/10/2022, 3:50:28 AM
2.192.6.100	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	2/10/2022, 3:42:39 AM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.6.26	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:52 AM
2.192.6.176	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:37 AM
2.192.7.117	b1daa07922bdca09ed41c7c595bebfcb800d22452fdf7f40a46a99d1289d1b36	1	2/9/2022, 10:14:26 PM
2.192.7.50	56081d5a3fb79ee327cbc6843a6f217db17b697535e41f3397d9380433fd7973	1	2/9/2022, 10:12:20 PM
2.192.7.66	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 10:09:46 PM
2.192.7.231	83a34fab143a111a251c9335f78b2cc74dfdc146e9b1d124487e2f4942187db9b	1	2/9/2022, 10:09:21 PM
2.192.7.96	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 10:07:21 PM
2.192.7.146	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/9/2022, 10:05:32 PM
2.192.7.42	57bd0384a64c64f63b986d5d82162cba311acc045ef9af0dcf1f13f5d8b6fef11	1	2/9/2022, 10:00:26 PM
2.192.7.116	d8664eaf6fba634791ff6d3b9ae26c0d6c21a4a5ac54868d58a243358ed12737a	1	2/9/2022, 9:59:01 PM
2.192.11.83	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc03264661f80d687484	1	2/9/2022, 9:41:54 PM
2.192.11.56	cc4a8a5280beac5f97de1fc9a8be98ad1781e3f1e7887accf7ad1239ef919729	1	2/9/2022, 9:41:51 PM
2.192.11.151	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc03264661f80d687484	1	2/9/2022, 9:39:46 PM
2.192.11.203	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/9/2022, 9:38:49 PM
2.192.11.167	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 9:25:09 PM
2.192.2.63	68327011912c6be3059a32c0f97e92be8297506cc927b1f641c74508ab7e55cc	1	2/9/2022, 8:45:58 PM
2.192.11.202	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	2/9/2022, 7:35:23 PM
2.192.9.26	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/9/2022, 7:27:05 PM
2.192.0.249	0b84d07fa94be76fc4a7b82a43a88b532b3d211031c10b8b49f3e40a5a507d4ae	1	2/9/2022, 4:55:42 PM
2.192.0.158	a3aa99d4c86db0b3f3bd7011e1ede7fcd109744e2fbbe6fb52bfdc94d3d3b055	1	2/9/2022, 4:43:04 PM
2.192.10.152	6ab09b14de3a32a30909a8c9e3ad7b3cd1487d208b9480c80ac01a8d86d60e476	1	2/9/2022, 4:19:19 PM
2.192.10.212	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 4:10:30 PM
2.192.7.25	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	2/9/2022, 9:20:17 AM
2.192.9.173	2ca23ad3a8a9ac5637054c6207db6d1f3b119b996f0dc47cfcca9c7847694cafa	1	2/9/2022, 12:40:31 AM
2.192.9.223	58e1488de43e5a4ed6872ff8961e61834cb17cb2315c305bed8d7eecf2cad0bb9	1	2/9/2022, 12:28:08 AM
2.192.9.222	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 12:26:57 AM
2.192.9.177	1e33fae1dfa19928f1d739b821fff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	2/9/2022, 12:21:47 AM
2.192.1.168	943be5cb86129d95ace9a15080fde86e301c0588023a288ca94cf945b9dc8c8f	1	2/8/2022, 10:18:33 PM
2.192.1.155	f18993e590db02cb92dc63335bd5fb96d40e5b68dd4bdc5dfa148959a0af356f	1	2/8/2022, 10:08:50 PM
2.192.1.162	30dd8cba5ababe04616399e56e9f7b46af5c9ab3fca5300e97bf84b80fcf5e14	1	2/8/2022, 10:08:27 PM
2.192.1.19	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:05:21 PM
2.192.1.207	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:04:11 PM
2.192.1.172	9c34af632db9569f9222b22fecc85a3cdb0a535dcdf55d4a2ec8dd26dc9ad855	1	2/8/2022, 10:03:30 PM
2.192.4.228	ee5e83ea61be05e0b8ef9782344d809abd1aabad10ac1019bf3aeaaa9a98d9af	1	2/8/2022, 9:52:11 PM
2.192.1.214	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	2/8/2022, 9:51:37 PM
2.192.1.53	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/8/2022, 9:51:35 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.4.159	d12345b3395500b077e84dd001866f7f6a102cd862d4d38d62e380988d57a15b0	1	2/8/2022, 9:43:48 PM
2.192.4.43	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 9:42:30 PM
2.192.4.215	0f514f8672d55cb9edefca40e9925d9fc36102b4ef5dcdcbb2a9c955eeadaa0e1	1	2/8/2022, 9:40:53 PM
2.192.0.43	ef72b5f1a1ac614a1e2c83b8a65201d87bcabe4ef16db340eb8705e709ae986e	1	2/8/2022, 8:39:59 PM
2.192.0.90	380fae1b309686b9703cd35fd31d75010f5187d4222c87f78da7e8c8053cbbf3c	1	2/8/2022, 8:28:58 PM
2.192.9.254	a6951a61b0adf3e54897349d17de9f0c3701f20012eee9a7170b1aaddf8e89b79	1	2/8/2022, 8:21:48 PM
2.192.8.65	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/8/2022, 6:56:34 PM
2.192.8.125	89a97163bcde6c961778080021438a05f89edee5ece21155aa408e1f1c1dc181	1	2/8/2022, 6:45:18 PM
2.192.9.145	94eaa1c54a054b484868342bd9e6d6ec5256e4ef2ec655b2063e438d814cb191	1	2/8/2022, 5:24:56 AM
2.192.1.106	4582ec1662f1266278eb33f68201e9665d8e3f7e8e0bfd4a5c2ce8e552ffd0f0	1	2/7/2022, 12:03:05 PM
2.192.10.69	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	2/7/2022, 11:06:41 AM
2.192.7.250	c9c98101f12f59134432c49ce306305c9314f941c9e9d3af1bca44bb7dc64cd8	1	2/7/2022, 5:01:21 AM

Certificate Without Revocation Control

-0.5 SCORE IMPACT

A certificate was observed that did not contain either CRL or OCSP URLs.

Description

When a Certificate Authority (CA) issues a certificate, they embed URLs that can be used to check if a certificate has been revoked. Certificates that are revoked are no longer valid, and TLS clients (e.g., web browsers) will refuse to connect to servers presenting revoked certificates.
Certificates are revoked for a variety of reasons: the decommissioning of a server, the retirement of a product or business name, the early renewal of a replacement certificate, or the belief that an attacker may have acquired the certificate's corresponding private key.
If a certificate does not include revocation controls, it cannot be revoked. Issuing irrevocable credentials is a violation of best practices.

Recommendation

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

194 findings

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.0.111	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/11/2022, 2:00:46 PM
2.192.1.99	495e762b5aa7fd9dd83c3947f94f0d91f0fd0a2722b346f07f2038ea4525f5f3	1	3/11/2022, 7:20:14 AM
2.192.1.171	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/11/2022, 7:16:49 AM
2.192.1.62	66c0195145de59bff811f7ccb3f9487a15f2a105dd98347ccfeb939c8521c5e6e	1	3/11/2022, 7:12:56 AM
2.192.1.149	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/11/2022, 7:03:49 AM
2.192.1.106	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 7:03:20 AM
2.192.1.60	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	3/11/2022, 6:55:28 AM
2.192.7.192	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 1:31:43 AM
2.192.2.247	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	3/10/2022, 7:57:13 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.2.167	ac3395fbaecd3bc28bd6420dc5d99a3eef1789819b45bdc0d60abe410a63559c9	1	3/10/2022, 7:43:19 PM
2.192.2.159	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/10/2022, 7:36:06 PM
2.192.0.92	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 7:33:33 PM
2.192.0.56	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 7:27:22 PM
2.192.0.29	995b3eedc0b73b2fd244a7dded51dbabfe1c22f1bc5a24b87cf9fa45aab2a46e7	1	3/10/2022, 7:22:56 PM
2.192.8.177	72403d4f01fccf8e13e830a61bb64004de11a58034b5be80947f6b81177a03b45	1	3/10/2022, 6:41:15 PM
2.192.8.23	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 6:37:48 PM
2.192.8.234	57ef50936a84664f41134c375c372c61917e1a9480436eeb19eb8ea074b43503	1	3/10/2022, 6:34:54 PM
2.192.3.216	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	3/10/2022, 4:43:15 PM
2.192.3.195	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 4:41:11 PM
2.192.3.58	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/10/2022, 4:37:17 PM
2.192.10.39	c415794f859abcb944bc8a7b168967a5963a0179d5d4b2d25dabf242dc7ffe03	1	3/10/2022, 4:04:36 PM
2.192.3.112	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 3:56:39 PM
2.192.1.141	bb826cd36f3b6f01458e391802a7068b3716f4c214de14760c95670f951abe53	1	3/10/2022, 11:37:01 AM
2.192.11.136	983033524ba5518ed3f22df894c80b06d14d792dffe3b275495d6e9a5ce76cf9c	1	3/10/2022, 7:29:28 AM
2.192.10.86	a6951a61b0adf3e54897349d17de9f0c3701f20012eee9a7170b1aaddf8e89b79	1	3/10/2022, 7:25:56 AM
2.192.11.62	ee5e83ea61be05e0b8ef9782344d809ab1d1aabad10ac1019bf3aeaaa9a98d9af	1	3/10/2022, 7:25:29 AM
2.192.11.209	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 7:20:47 AM
2.192.11.106	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	3/10/2022, 7:15:35 AM
2.192.11.21	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 7:14:51 AM
2.192.7.68	3d42db219fb46a96b8223836774b054f5514a5f5daded827e5c63bb5641793f4c	1	3/10/2022, 6:54:51 AM
2.192.7.247	bd503c3b956fd2f76fd80b8e11100909b064dcb30f629e3e6b06c997416b862b	1	3/10/2022, 6:47:41 AM
2.192.7.62	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 6:37:23 AM
2.192.10.171	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/10/2022, 6:34:21 AM
2.192.10.53	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 6:31:04 AM
2.192.11.229	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	3/10/2022, 6:26:17 AM
2.192.10.83	73f052bda7fd485dc767a3018fa9ef819cc1c20c88c9224768554c5182f30506	1	3/10/2022, 6:18:55 AM
2.192.10.65	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc03264661f80d687484	1	3/10/2022, 6:17:09 AM
2.192.11.223	bf1ca590b3cc538370ee30d21debd52f7f513e3057a15b14d511f0532899c9a2a	1	3/10/2022, 6:16:39 AM
2.192.11.111	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 6:15:47 AM
2.192.2.0	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	3/10/2022, 5:56:59 AM
2.192.6.165	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 4:38:09 AM
2.192.5.79	2b88cd6a6862e630db53858fd905a1911fc8ba1139ceddc11cce0bc7394c2e83	1	3/10/2022, 4:20:25 AM
2.192.5.239	ef1fd069e6f4fa81e139cb39d0bb049cca48e49808a04193e4674667089d1343	1	3/10/2022, 3:58:57 AM
2.192.6.13	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 3:55:12 AM
2.192.5.158	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 3:53:36 AM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.5.166	1036a96b07223f3ac421e92f3f3f1221ee89198ff875c1e3448c870bbb6d881f2	1	3/10/2022, 3:46:45 AM
2.192.5.199	6be36afe45749ce202b1d2ba52e9dd30e14e2dafdf4872b391650d18fe20fd7e0	1	3/10/2022, 3:39:54 AM
2.192.2.118	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/9/2022, 9:10:26 PM
2.192.2.80	f79bb73f856f690b2a8396b18ca22480023161636760e586149949bccff03f52	1	3/9/2022, 9:05:48 PM
2.192.2.18	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	3/9/2022, 8:55:31 PM
2.192.2.84	f29873c163f46c21d383ab714ae615fc55b5d4c0f85f966120471888e33afcc1	1	3/9/2022, 8:55:28 PM
2.192.2.171	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/9/2022, 8:54:18 PM
2.192.2.175	a9ddd4aa8b5c6049d87b2654e2326244 4f91befda60c7a4c3d8bc8ed6aff417b	1	3/9/2022, 8:51:05 PM
2.192.4.141	49a9d29d80d87b8ecc3a7874585d07f3953cf9d0dfd465169eaa87abcacd9dee	1	3/9/2022, 6:59:45 PM
2.192.4.253	b26beb56f515052d6a9e7db1f34d24c7b9dba533c54adc60782dcb2682e27566	1	3/9/2022, 6:49:32 PM
2.192.1.4	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/9/2022, 5:50:43 AM
2.192.0.236	c0a50cd4f6db9282bb7547f9787e007f691448a3af15c37c566359496d5eb446a	1	3/9/2022, 5:49:42 AM
2.192.0.234	be8aaaad93b39f9007a5ac6fadf236616f3d38b3dbba258b36bc2d2c80703e01	1	3/9/2022, 5:47:27 AM
2.192.0.133	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 5:46:21 AM
2.192.0.200	0eab86098cbc361b52a1280144d07c4a5515880700c98a18d0679571e795468a7	1	3/9/2022, 5:43:56 AM
2.192.0.189	0f3a7e2632f01e451aa855139f108ef65fc8c1d6128cd7d84cea0436cbab8d81	1	3/9/2022, 5:41:40 AM
2.192.0.211	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/9/2022, 5:28:35 AM
2.192.7.148	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/9/2022, 4:23:34 AM
2.192.6.55	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 2:02:00 AM
2.192.6.23	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	3/9/2022, 1:51:10 AM
2.192.6.242	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 1:48:02 AM
2.192.7.7	1d6b73c5b8c91774e7a2a993759d71ebd1846c0fb6234f5a167e574eadd40312	1	3/9/2022, 1:43:46 AM
2.192.6.218	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/9/2022, 1:37:44 AM
2.192.6.54	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/9/2022, 1:37:35 AM
2.192.5.128	d8664eaf6fba634791ff6d3b9ae26c0d6c21a4a5ac54868d58a243358ed12737a	1	3/9/2022, 12:55:57 AM
2.192.9.143	cc4a8a5280beac5f97de1fc9a8be98ad1781e3f1e7887accf7ad1239ef919729	1	3/8/2022, 6:59:13 PM
2.192.4.164	b1b10ab845619a6cd7043a5f651dd3c9ac44f04e4041d9ba17d8a948ace14f2f	1	3/8/2022, 6:51:10 PM
2.192.9.236	15e291ef2b9d8a5316714c3a48898e9abfb207bd90fb287d3ef2dab747183daa3	2	3/8/2022, 6:49:22 PM
2.192.9.125	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:48:03 PM
2.192.4.34	7905ac7ab222693a18abc2bad129e1dc91918f5ec61faf3f82c64e3d6becaac1d	1	3/8/2022, 6:47:24 PM
2.192.9.126	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:46:48 PM
2.192.9.199	e45500a6cb74a7dc30628d79e4ec4ba9fa7dd0fe404b270b249e766a61d6ac82	1	3/8/2022, 6:45:50 PM
2.192.4.48	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:45:11 PM
2.192.4.56	8326ae91ce47c1fe8cde06073bb928028e14eb1e3c11267125e789e333f37a1d6	1	3/8/2022, 6:42:42 PM
2.192.10.6	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:34:25 PM
2.192.4.41	94eaa1c54a054b484868342bd9e6d6ec5256e4ef2ec655b2063e438d814cb191	1	3/8/2022, 6:34:21 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.9.144	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/8/2022, 6:11:38 PM
2.192.9.104	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	3/8/2022, 6:11:35 PM
2.192.9.112	743f6840b846750b764eb65a556ae1e2b183862ab59ee0e5388e06a9c0f3297f2	1	3/8/2022, 6:05:08 PM
2.192.10.132	68327011912c6be3059a32c0f97e92be8297506cc927b1f641c74508ab7e55cc	1	3/6/2022, 1:23:47 AM
2.192.0.202	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/6/2022, 12:19:31 AM
2.192.11.17	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	2/24/2022, 9:48:40 PM
2.192.11.60	7004dc9d03491de605818a4382fce5b8b17ff0c50e2a5d928d3f437dde1968cd6	1	2/24/2022, 9:00:27 PM
2.192.5.9	0bdaee6af1262fef5d0f03dd02f7efcd540974e0b6bf6d2ef8a5167213560474	1	2/23/2022, 10:19:49 PM
2.192.7.50	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	2/23/2022, 12:58:43 AM
2.192.5.162	5ddcd1559efb72079b654485c66c18acafe134606b9bda30b2fbe9cb44fa455c6	1	2/22/2022, 3:13:55 AM
2.192.6.117	d0616a7224a8f6d34a4c1c4fc1e5398183e3069674a8b64f78204cb41eb1b879	1	2/20/2022, 10:54:17 PM
2.192.4.117	974a16997ca42b9731f50d2d727fa6bca70190c865357b0003b52a0bd307c4a8	1	2/18/2022, 3:51:33 PM
2.192.0.37	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/18/2022, 8:24:46 AM
2.192.1.157	4e31dfe1eb03f38e7122e2702937911a12cbd67f556ae3351f58d43d8cf02e96	1	2/18/2022, 8:02:56 AM
2.192.5.164	75eb15acbf13d4c39766110f766d2cb0369034603ddc2548b4d284d30243f0cd	1	2/18/2022, 6:53:52 AM
2.192.2.34	1036a96b07223f3ac421e92f3f3f1221ee8998ff875c1e3448c870bbb6d881f2	1	2/16/2022, 6:19:52 AM
2.192.11.5	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 1:07:54 PM
2.192.10.229	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 1:05:41 PM
2.192.4.228	4fec42fbb2a17a39e02c9a03e24d5e7a54e715b964cfb2fd8231367ea4a7fade	1	2/15/2022, 10:31:41 AM
2.192.6.143	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 10:04:50 AM
2.192.9.145	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 9:28:06 AM
2.192.9.144	13dcd3ff251061088dfe72eb3006978677315902 2d9a90d1a2d30655e1ad24382	1	2/15/2022, 9:28:05 AM
2.192.0.44	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 9:19:40 AM
2.192.4.109	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 6:47:55 AM
2.192.8.94	c4a148013f7b023b84b003e316626c52cbe5ea128a378beabb1a19254073ff2d	1	2/15/2022, 2:19:50 AM
2.192.11.151	dee7de7afac7a23fe1624fb3670f5c25a4102268b7643dc03264661f80d687484	2	2/12/2022, 4:56:25 AM
2.192.10.36	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	2/11/2022, 10:33:43 AM
2.192.5.162	7905ac7ab222693a18abc2bad129e1dc91918f5ec61faf3f82c64e3d6becaac1d	1	2/11/2022, 10:05:12 AM
2.192.5.172	6f503ea0843c3228b3704cce7c4c6f1e3e14421ed960ce8260506c959bd841e86	1	2/11/2022, 10:00:41 AM
2.192.4.237	af10a28e8fc466dc62a2aa6247ec5b1daec8b77e9cf0bb5ecf54ecc57da91fee	1	2/11/2022, 9:56:44 AM
2.192.5.58	80e089dd74979ae84d9a2e1b45c698726adafcec4c6ca183b9f3f7f0cdb2e542	1	2/11/2022, 9:55:34 AM
2.192.5.182	a9ddd4aa8b5c6049d87b2654e2326244 4f91befda60c7a4c3d8bc8ed6aff417b	1	2/11/2022, 9:51:02 AM
2.192.4.185	7f621bb6fa2ad11096c354dad397b3d6fc711737fee400c0f3a92d3bf991f6403	1	2/11/2022, 9:48:04 AM
2.192.2.174	c80b2e6bf2c33cd85bbb2220a301f3ccc0101e43355de8cff04b1274eb6f85414	1	2/11/2022, 9:39:12 AM
2.192.6.252	ec0b77d7cb90e1f175b7fbf332cf331ff11cd610b4f894dbed128f8db7a052bbe	1	2/11/2022, 6:34:02 AM
2.192.6.118	728a52efa109420a1c892041e9637280e43b3d7f4547435e24bab02b6cd3aff6	1	2/11/2022, 6:23:45 AM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.6.243	3fea6e1fdc8aeac6463615badb58eaccc4c1c2b092e27bdd1693adf1250189741	1	2/11/2022, 6:23:37 AM
2.192.11.69	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/11/2022, 12:16:45 AM
2.192.3.159	1172d82213af66fba30f80af18572648b2d38b524e238206bde88a131892ea78	1	2/10/2022, 11:09:44 PM
2.192.3.121	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	2/10/2022, 11:05:03 PM
2.192.3.75	27d8bf86ebc677f9455c823cecab4c800ac32f47abacac38962cfc04417525be	2	2/10/2022, 11:02:42 PM
2.192.3.232	8c4129a0634eba1a1d341815ef59f64b6a5c1d03ad0ede85e9f31e29545dce082	1	2/10/2022, 11:02:29 PM
2.192.3.142	2c4ff0142914b45174c478d1ac5347279eb5edbb2dc37d6fe180b6511fe989c8	1	2/10/2022, 11:02:18 PM
2.192.3.100	85eb21e49e9d8b2797747dffde96ba01236bd9c14e6b0ae1e6c7b544c706bf44	1	2/10/2022, 11:01:28 PM
2.192.3.135	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 11:01:16 PM
2.192.3.59	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/10/2022, 10:56:12 PM
2.192.0.38	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 8:13:33 PM
2.192.0.250	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	2/10/2022, 8:03:45 PM
2.192.0.100	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/10/2022, 8:02:09 PM
2.192.0.155	00cf2c6fdad819da6310cbd9b5a53ea5c37366dcc2c529f3683203f8bcf09cca	1	2/10/2022, 8:02:02 PM
2.192.0.79	49a9d29d80d87b8ecc3a7874585d07f3953cf9d0dfd465169eaa87abcacd9dee	1	2/10/2022, 7:54:03 PM
2.192.10.64	547ff655f1ef78800409f359730bc20f737e3a566e8eabb3a0106586c100aca2	1	2/10/2022, 7:53:51 PM
2.192.10.73	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 7:47:50 PM
2.192.4.221	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	2/10/2022, 12:42:26 PM
2.192.5.250	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 6:45:29 AM
2.192.6.3	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/10/2022, 6:39:53 AM
2.192.6.210	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	2/10/2022, 3:50:28 AM
2.192.6.174	f19a54f29e8fb7ad7392da3f74dffb2ac48ae6ac27a796d3b02883fa17a1b9e1	1	2/10/2022, 3:44:04 AM
2.192.6.100	98b4742f431440761c7fd201eec206c4466113ca0b3beee347d56f04cf792e89f4	1	2/10/2022, 3:42:39 AM
2.192.6.26	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:52 AM
2.192.6.176	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:37 AM
2.192.11.49	995b3eedc0b73b2fd244a7dded51dbabfe1c22f1bc5a24b87cf9fa45aab2a46e7	1	2/10/2022, 2:08:51 AM
2.192.7.117	b1daa07922bdca09ed41c7c595bebfcb800d22452fdf7f40a46a99d1289d1b36	1	2/9/2022, 10:14:26 PM
2.192.7.50	56081d5a3fb79ee327cbc6843a6f217db17b697535e41f3397d9380433fd7973	1	2/9/2022, 10:12:20 PM
2.192.7.66	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 10:09:46 PM
2.192.7.231	83a34fab143a111a251c9335f78b2cc74dfdc146e9b1d124487e2f4942187db9b	1	2/9/2022, 10:09:21 PM
2.192.7.96	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 10:07:21 PM
2.192.7.146	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/9/2022, 10:05:32 PM
2.192.7.42	57bd0384a64c64f63b986d5d82162cba311acc045ef9af0dcf1f13f5d8b6fef11	1	2/9/2022, 10:00:26 PM
2.192.7.116	d8664eaf6fba634791ff6d3b9ae26c0d6c21a4a5ac54868d58a243358ed12737a	1	2/9/2022, 9:59:01 PM
2.192.11.83	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc03264661f80d687484	1	2/9/2022, 9:41:54 PM
2.192.11.56	cc4a8a5280beac5f97de1fc9a8be98ad1781e3f1e7887accf7ad1239ef919729	1	2/9/2022, 9:41:51 PM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.11.203	e002709f07e7e9e40342e6c26909092e cfd6cd9f3b3d032da6e20e0ee89cadce	1	2/9/2022, 9:38:49 PM
2.192.11.152	8af33dfb83ded5ac775eacedde04d08c6c1 85cf5b5bea02fcebc90b60c59772f9	1	2/9/2022, 9:33:13 PM
2.192.11.167	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 9:25:09 PM
2.192.2.63	68327011912c6be3059a32c0f97e92be82 97506cc927b1f641c74508ab7e55cc	1	2/9/2022, 8:45:58 PM
2.192.11.202	6831970d31c8b170ab443da794bc84da27 3f3a120ae76fddbed757a1d7db63b5	1	2/9/2022, 7:35:23 PM
2.192.9.26	8a6511e0835f5bbd71a34a273c91d5cabd3 0af2a79e3b88a103a6f61c34691d0	1	2/9/2022, 7:27:05 PM
2.192.0.249	0b84d07fa94be76fc4a7b82a43a88b532b3 d211031c10b8b49f3e40a5a507d4ae		2/9/2022, 4:55:42 PM
2.192.0.158	a3aa99d4c86db0b3f3bd7011e1ede7fcd10 9744e2fbbe6fb52bfdc94d3d3b055	1	2/9/2022, 4:43:04 PM
2.192.10.152	6ab09b14de3a32a30909a8c9e3ad7b3cd 487d208b9480c80ac01a8d86d60e476	1	2/9/2022, 4:19:19 PM
2.192.10.212	6158658b038a8ad15445d27c44c2c7282a1 bb609d5f5a978b7970fb37bb6a61a2		2/9/2022, 4:10:30 PM
2.192.7.25	98b4742f431440761c7fd201eec206c44661 3ca0b3beee347d56f04cf792e89f4		2/9/2022, 9:20:17 AM
2.192.9.173	2ca23ad3a8a9ac5637054c6207db6d1f3b2 19b996f0dc47cfcca9c7847694cafa	2	2/9/2022, 12:40:31 AM
2.192.9.223	58e1488de43e5a4ed6872ff8961e61834cb1 7cb2315c305bed8d7eecf2cad0bb9		2/9/2022, 12:28:08 AM
2.192.9.222	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 12:26:57 AM
2.192.9.177	1e33fae1dfa19928f1d739b821ff9f14c5bc98 5fe746e20f1510a1eea3d8ed7b	1	2/9/2022, 12:21:47 AM
2.192.1.168	943be5cb86129d95ace9a15080fde86e3 01c0588023a288ca94cf945b9dc8c8f	1	2/8/2022, 10:18:33 PM
2.192.1.155	f18993e590db02cb92dc63335bd5fb96d 40e5b68dd4bdc5dfa148959a0af356f	1	2/8/2022, 10:08:50 PM
2.192.1.162	30dd8cba5ababe04616399e56e9f7b46af 5c9ab3fca5300e97bf84b80fcf5e14	1	2/8/2022, 10:08:27 PM
2.192.1.19	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:05:21 PM
2.192.1.207	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:04:11 PM
2.192.1.172	9c34af632db9569f9222b22fecc85a3cdb 0a535dcdf55d4a2ec8dd26dc9ad855	1	2/8/2022, 10:03:30 PM
2.192.4.228	ee5e83ea61be05e0b8ef9782344d809ab d1aabad10ac1019bf3aeaaa9a98d9af	1	2/8/2022, 9:52:11 PM
2.192.1.214	bbecca6f745bc239331bd4b3cee07493d51 04ee0965a055a04f487fc9141baf6d		2/8/2022, 9:51:37 PM
2.192.1.53	e002709f07e7e9e40342e6c26909092e cfd6cd9f3b3d032da6e20e0ee89cadce	1	2/8/2022, 9:51:35 PM
2.192.4.73	2c4736a7c6a2e980a5610a2437fa6994bd df362c5345eb5055869b953af54174	1	2/8/2022, 9:45:28 PM
2.192.4.159	d12345b3395500b077e84dd001866f7f6a1 02cd862d4d38d62e380988d57a15b0		2/8/2022, 9:43:48 PM
2.192.4.43	47afbbb22314b00901c4524b601ae8d587 975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 9:42:30 PM
2.192.4.215	0f514f8672d55cb9edefca40e9925d9fc361 02b4ef5dcdcbb2a9c955eeadaa0e1		2/8/2022, 9:40:53 PM
2.192.0.43	ef72b5f1a1ac614a1e2c83b8a65201d87bca be4ef16db340eb8705e709ae986e	1	2/8/2022, 8:39:59 PM
2.192.0.90	380fae1b309686b9703cd35fd31d75010f51 87d4222c87f78da7e8c8053cbbf3c		2/8/2022, 8:28:58 PM
2.192.9.254	a6951a61b0adf3e54897349d17de9f0c3701 f20012eee9a7170b1aaddf8e89b79		2/8/2022, 8:21:48 PM
2.192.8.65	c7fd6d5d51e06ba71fea12d27f8e646b1d7f ecd845c5d50f584949b0fa58dfd3	1	2/8/2022, 6:56:34 PM
2.192.8.230	b1b10ab845619a6cd7043a5f651dd3c9ac4 4f04e4041d9ba17d8a948ace14f2f	1	2/8/2022, 6:54:10 PM
2.192.8.175	b37d66a37f48fbdd7949e48442836393d cc10f9511507f663a8d4fc59b48cb79	1	2/8/2022, 6:48:07 PM
2.192.8.125	89a97163bcde6c961778080021438a05f8 9edee5ece21155aa408e1f1c1dc181	1	2/8/2022, 6:45:18 PM
2.192.9.145	94eaa1c54a054b484868342bd9e6d6ec5 256e4ef2ec655b2063e438d814cb191	1	2/8/2022, 5:24:56 AM

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.9.120	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	2/7/2022, 12:52:38 PM
2.192.9.120	17ee951b02179879c7a49170cc02ab0645b1e8ee8667b2896875f39266d925d6	1	2/7/2022, 12:52:38 PM
2.192.1.106	4582ec1662f1266278eb33f68201e9665d8e3f7e8e0bfd4a5c2ce8e552ffd0f0	1	2/7/2022, 12:03:05 PM
2.192.10.69	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	2/7/2022, 11:06:41 AM
2.192.7.250	c9c98101f12f59134432c49ce306305c9314f941c9e9d3af1bca44bb7dc64cd8	1	2/7/2022, 5:01:21 AM

Industrial Control System Device Accessible

-1.3 SCORE IMPACT

We observed an industrial control system (ICS) device publicly exposed.

Description
Supervisory control and data acquisition (SCADA) and industrial control system (ICS) devices manage sensitive physical processes using data signals. Exposing them to the internet carries inherent risks that could compromise organizations and jeopardize human lives. ICS devices control critical infrastructure, such as power grid substations, manufacturing lines, sensors, and programmable logic controllers (PLCs), including relays and reclosers. These devices use a range of protocols, such as Modbus, DNP3, IEC-204, EtherNet/IP, Niagara Fox, BACNET, Omron, and PCWorx. Prioritize the removal of any exposed SCADA or ICS device from the public Internet and move it behind a VPN or firewall, as most critical infrastructure organizations do.

Recommendation
Review the business necessity of exposing an ICS device, such as Modbus, DNP3, BACNET, or other critical infrastructure devices. Place such devices behind a VPN or firewall. If it is not possible to remove the service from the internet, consider restricting the service by adding dependent IPs to an allow list.

3 findings

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
Siemens S7 PLC		2.192.3.67	102	2/21/2022, 6:55:21 AM
Modbus Device		2.192.0.178	502	2/13/2022, 12:23:53 PM
Tridium Niagara	3.8.38.7	2.192.9.177	1911	2/12/2022, 9:00:13 AM

HTTP Proxy Service Detected

We detected an HTTP proxy service exposed to the internet.

Description
A proxy server acts as an intermediary between a client, such as a web browser, requesting a resource and the server providing that resource. The use of a proxy server provides benefits such as load balancing, privacy, and security. However, it also introduces potential risks, such as increased likelihood of malware attacks, spam, display ads, unwanted software downloads, or other malicious traffic. Proxy servers do not encrypt data, so cybercriminals can intercept it.

Recommendation
Verify whether the HTTP proxy service has a legitimate use. Otherwise, remove it from your network.

3 findings

IP ADDRESS	PORT	LAST OBSERVED
2.192.9.42	8080	2/24/2022, 3:51:55 PM
2.192.6.50	8080	2/24/2022, 1:44:41 AM
2.192.9.89	8080	2/20/2022, 10:31:30 PM

Remote Access Service Observed

-0.3 SCORE IMPACT

We observed a remote access service or device publicly exposed.

Description
Remote access services allow users to reach endpoints on a network (separate of RDP/X11/VNC) with Microsoft Windows-Based Terminal (WBT). This server is used for Windows Remote Desktop and Remote Assistance connections, or router login services, such as TP-LINK/CPE/ActionTec TR-069. These devices can be a security risk and enable an entry point into a network by attackers.

Recommendation
This issue type concerns a remote access service, such as a router providing a remote login service, or a Windows server providing a remote assistance service. Examine devices on a case-by-case basis, restrict access to these devices to either authorized VPN connections or IP restrictions.

1 finding

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Microsoft Terminal Services	2.192.9.120	3389	2/7/2022, 12:52:38 PM

SSL/TLS Service Supports Weak Protocol

-1.9 SCORE IMPACT

A TLS service was observed supporting weak protocols.

Description
Transport Layer Security (TLS), the successor to Secure Socket Layer (SSL), is a network protocol that encrypt communications between TLS servers (e.g., websites) and TLS clients (e.g., web browsers). Every communication is secured by a cipher suite: a combination of several algorithms working in concert. Networking protocols do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. Consensus on which protocols are untrustworthy evolves over time, and if communications are sent with a weak protocol then that communication can be altered or decrypted.

Recommendation
Disable the protocols listed in the evidence column of the measurement.

17 findings

TARGET	PORT	OBSERVATIONS	LAST OBSERVED
2.192.1.106	443	1	3/11/2022, 7:03:26 AM
2.192.7.192	443	1	3/11/2022, 1:31:51 AM
2.192.3.195	443	1	3/10/2022, 4:41:19 PM
2.192.11.21	443	1	3/10/2022, 7:15:00 AM
2.192.11.111	443	1	3/10/2022, 6:15:56 AM
2.192.2.118	443	1	3/9/2022, 9:10:35 PM
2.192.6.23	443	1	3/9/2022, 1:51:32 AM
2.192.7.7	443	1	3/9/2022, 1:44:05 AM
2.192.4.34	443	1	3/8/2022, 6:47:27 PM
2.192.5.162	443	1	2/11/2022, 10:05:15 AM
2.192.6.118	443	1	2/11/2022, 6:23:53 AM
2.192.3.142	443	1	2/10/2022, 11:02:22 PM
2.192.0.100	443	1	2/10/2022, 8:02:49 PM
2.192.6.3	443	1	2/10/2022, 6:40:01 AM
2.192.11.203	443	1	2/9/2022, 9:38:58 PM
2.192.1.53	443	1	2/8/2022, 9:51:43 PM
2.192.8.65	443	1	2/8/2022, 6:57:11 PM

Embedded IOT Web Server Exposed

We detected an embedded IOT web server exposed to the internet.

Description

Recommendation

The internet of things (IoT) involves deployment of web-based services that communicate with, and control, devices such as appliances, cameras, or light fixtures. The technology entails a growing number of security concerns, such as weak authentication, inconsistent security updates, and unencrypted communication between devices. Exploits such as SQL injections, man-in-the-middle attacks, and native code injection on IOT devices are possible and common. Additionally, the data exchanged between devices is at risk. Exposing an IOT service to the internet compounds these risks by widening access for malicious parties.

Place the IOT web server behind a firewall.

1 finding

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
Mongoose httpd	3.7	2.192.5.162	443	2/13/2022, 3:57:31 AM

Networking Service Observed

We observed a networking service or device publicly exposed.

Description
Networking services and devices provide core capabilities to orchestrate the flow and performance of network traffic, and enforce its security. These services include BGP, TRAM (router firmware update service), point-to-point protocol service, WAN management, and bandwidth testing. Devices include large internetwork routers, such as Cisco, Quagga, Zebra, and Juniper; firewalls, such as Cisco Meraki; and home routers. These devices do not pose an inherent security risk, but knowing they exist helps make your digital footprint more complete.

Recommendation
This issue type concerns a networking service or device, such as a router or service that is associated with routers like BGP, a firewall, or tunneling service. No change or update to your internet-facing assets is necessary.

3 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
MikroTik bandwidth-test server	2.192.9.72	2000	3/8/2022, 8:51:27 AM
MikroTik bandwidth-test server	2.192.4.218	2000	2/18/2022, 5:08:11 PM
MikroTik bandwidth-test server	2.192.0.131	2000	2/18/2022, 11:49:43 AM

FTP Service Observed

-0.3 SCORE IMPACT

We observed FTP, a file-sharing service, publicly exposed.

Description
The FTP protocol offers access to files stored on servers, giving users the ability to upload, download, and delete files. Many FTP servers are used by automated processes, and are neglected or poorly-configured. Modern protocols, such as SFTP, provide better security than FTP.
We observed an FTP service on the Internet, accessible by the public. File-sharing services are attractive targets to attackers due to the data they may contain. An attacker that gains access to the files on an FTP server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached FTP server may result in legal proceedings, have public notification requirements, negatively impact public image, and have insurance implications.
Attackers may target the service with authentication bypass

Recommendation
Review the business necessity of hosting a public FTP server, and remove it from the Internet if possible. If not possible, consider restricting the service by allowlisting the IP addresses that require access.

attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Attackers may launch denial-of-service (DoS) attacks against the service, rendering it unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

30 findings

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
vsftpd	3.0.3	2.192.1.62	21	3/7/2022, 8:54:23 PM
ProFTPD or KnFTPD		2.192.1.119	21	3/7/2022, 8:53:38 PM
oftpd		2.192.1.63	21	3/7/2022, 8:51:06 PM
ProFTPD	1.3.5rc4	2.192.3.159	21	3/7/2022, 6:15:31 PM
ProFTPD		2.192.3.85	21	3/7/2022, 6:10:54 PM
ProFTPD		2.192.3.67	21	3/7/2022, 6:10:38 PM
MikroTik router ftpd	6.48.1	2.192.1.236	21	3/7/2022, 5:26:28 PM
ProFTPD		2.192.7.217	21	3/7/2022, 4:31:11 PM
		2.192.10.171	21	3/7/2022, 4:31:07 PM
ProFTPD	1.3.5rc4	2.192.10.65	21	3/7/2022, 4:28:35 PM
ProFTPD		2.192.5.105	21	3/7/2022, 4:04:21 PM
vsftpd	2.0.8 or later	2.192.2.175	21	3/7/2022, 2:49:30 PM
vsftpd	2.0.5	2.192.0.54	21	3/7/2022, 12:04:19 PM
MikroTik router ftpd	6.48.1	2.192.9.72	21	3/7/2022, 10:09:41 AM
vsftpd	2.0.8 or later	2.192.4.146	21	3/7/2022, 10:09:18 AM
vsftpd	3.0.3	2.192.4.43	21	3/7/2022, 10:09:00 AM
vsftpd	2.0.8 or later	2.192.4.31	21	3/5/2022, 9:11:37 PM
AVM FRITZ!Box ftpd		2.192.11.60	4117	2/24/2022, 9:00:27 PM
vsftpd (before 2.0.8) or WU-FTPD		2.192.3.100	21	2/24/2022, 4:08:27 PM
MikroTik router ftpd	6.48.1	2.192.0.161	21	2/7/2022, 7:01:13 PM
vsftpd	2.0.8 or later	2.192.10.148	21	2/7/2022, 6:58:36 PM
MikroTik router ftpd	6.48.1	2.192.4.32	21	2/7/2022, 5:45:41 PM
ProFTPD	1.3.5rc4	2.192.11.83	21	2/7/2022, 3:12:14 PM
vsftpd	2.0.8 or later	2.192.11.218	21	2/7/2022, 3:09:36 PM
vsftpd	2.0.5	2.192.1.18	21	2/7/2022, 2:31:45 PM
		2.192.0.200	21	2/7/2022, 2:18:46 PM
ProFTPD		2.192.0.48	21	2/7/2022, 2:15:14 PM
MikroTik router ftpd	6.48.1	2.192.7.36	21	2/7/2022, 11:41:11 AM
ProFTPD		2.192.9.73	21	2/7/2022, 11:30:04 AM
vsftpd	2.0.8 or later	2.192.9.190	21	2/7/2022, 11:30:00 AM

TLS Service Supports Weak Cipher Suite

-1.2 SCORE IMPACT

A TLS service was observed supporting weak cipher suites.

Description
Transport Layer Security (TLS), the successor to Secure Socket Layer (SSL), is a network protocol that encrypt communications between TLS servers (e.g., websites) and TLS clients (e.g., web browsers). Every communication is secured by a cipher suite: a combination of several algorithms working in concert. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. Consensus on which algorithms are untrustworthy evolves over time, and if a communication is protected with a weak cipher suite then that communication can be altered or decrypted.

Recommendation
Disable the cipher suites listed in the evidence column of the measurement.

61 findings

TARGET	PORT	OBSERVATIONS	LAST OBSERVED
2.192.1.42	443	1	3/11/2022, 7:10:44 AM
2.192.1.106	443	1	3/11/2022, 7:03:26 AM
2.192.1.60	443	1	3/11/2022, 6:55:58 AM
2.192.7.192	443	1	3/11/2022, 1:31:51 AM
2.192.3.195	443	1	3/10/2022, 4:41:19 PM

TARGET	PORT	OBSERVATIONS	LAST OBSERVED
2.192.3.112	443	1	3/10/2022, 3:56:42 PM
2.192.10.86	443	1	3/10/2022, 7:26:26 AM
2.192.11.21	443	1	3/10/2022, 7:15:00 AM
2.192.10.83	443	1	3/10/2022, 6:19:01 AM
2.192.11.111	443	1	3/10/2022, 6:15:56 AM
2.192.5.199	443	1	3/10/2022, 3:39:56 AM
2.192.2.118	443	1	3/9/2022, 9:10:35 PM
2.192.2.120	443	1	3/9/2022, 9:03:09 PM
2.192.2.84	443	1	3/9/2022, 8:55:32 PM
2.192.4.31	443	1	3/9/2022, 6:53:11 PM
2.192.0.206	443	1	3/9/2022, 5:46:46 AM
2.192.0.133	443	1	3/9/2022, 5:46:40 AM
2.192.0.189	443	1	3/9/2022, 5:41:48 AM
2.192.6.23	443	1	3/9/2022, 1:51:32 AM
2.192.6.242	443	1	3/9/2022, 1:48:17 AM
2.192.7.7	443	1	3/9/2022, 1:44:05 AM
2.192.5.168	443	1	3/9/2022, 1:10:13 AM
2.192.4.164	443	1	3/8/2022, 6:51:16 PM
2.192.4.34	443	1	3/8/2022, 6:47:27 PM
2.192.9.37	443	1	3/8/2022, 6:44:41 PM
2.192.4.56	443	1	3/8/2022, 6:42:45 PM
2.192.4.60	443	1	3/8/2022, 6:42:06 PM
2.192.4.146	443	1	3/8/2022, 6:39:24 PM
2.192.6.174	443	2	2/17/2022, 4:11:45 PM
2.192.10.229	8443	1	2/15/2022, 1:05:48 PM
2.192.9.145	8443	1	2/15/2022, 9:28:15 AM
2.192.4.109	8443	1	2/15/2022, 6:48:04 AM
2.192.1.52	443	1	2/11/2022, 12:34:07 PM
2.192.2.0	443	1	2/11/2022, 10:54:01 AM
2.192.5.162	443	1	2/11/2022, 10:05:15 AM
2.192.4.201	443	1	2/11/2022, 10:02:10 AM
2.192.4.185	443	1	2/11/2022, 9:48:34 AM
2.192.6.118	443	1	2/11/2022, 6:23:53 AM
2.192.3.142	443	1	2/10/2022, 11:02:22 PM
2.192.3.59	443	1	2/10/2022, 10:56:30 PM
2.192.0.250	443	1	2/10/2022, 8:04:15 PM
2.192.0.100	443	1	2/10/2022, 8:02:49 PM
2.192.0.155	443	1	2/10/2022, 8:02:12 PM
2.192.0.44	443	1	2/10/2022, 8:00:57 PM
2.192.11.5	443	1	2/10/2022, 7:58:32 PM
2.192.6.3	443	1	2/10/2022, 6:40:01 AM
2.192.11.225	443	1	2/10/2022, 2:15:45 AM
2.192.7.50	443	1	2/9/2022, 10:14:12 PM
2.192.11.203	443	1	2/9/2022, 9:38:58 PM
2.192.11.142	443	1	2/9/2022, 9:35:57 PM
2.192.11.152	443	1	2/9/2022, 9:33:18 PM
2.192.11.167	443	1	2/9/2022, 9:25:12 PM
2.192.8.32	443	1	2/9/2022, 6:49:58 PM
2.192.9.222	443	1	2/9/2022, 12:26:59 AM
2.192.1.53	443	1	2/8/2022, 9:51:43 PM
2.192.4.73	443	1	2/8/2022, 9:45:31 PM
2.192.0.90	443	1	2/8/2022, 8:29:05 PM
2.192.9.254	443	1	2/8/2022, 8:22:18 PM
2.192.8.65	443	1	2/8/2022, 6:57:11 PM
2.192.8.230	443	1	2/8/2022, 6:54:16 PM
2.192.8.175	443	1	2/8/2022, 6:48:11 PM

! Certificate Lifetime Is Longer Than Best Practices

-0.5 SCORE IMPACT

A certificate was observed with a validity period longer than dictated by the CAB forum's baseline requirements.

Description

When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. The Certificate Authority and Browser (CAB) Forum, an industry group that sets standards surrounding the creation and use of certificates, regularly

Recommendation

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

publishes updates to a document called the Baseline Requirements (BR). Roughly every two years the BR is updated to reduce the maximum validity period of certificates issued after a certain date. Older certificates have longer validity periods, but certificates issued after September 1, 2020 should have validity periods no longer than 398 days.

111 findings

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.0.111	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/11/2022, 2:00:46 PM
Evidence : 730d >= 398d			
2.192.1.99	495e762b5aa7fd9dd83c3947f94f0d91f0fd0a2722b346f07f2038ea4525f5f3	1	3/11/2022, 7:20:14 AM
Evidence : 1095d >= 825d			
2.192.1.106	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 7:03:20 AM
Evidence : 9999d >= 60mo			
2.192.7.192	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/11/2022, 1:31:43 AM
Evidence : 9999d >= 60mo			
2.192.2.247	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d		3/10/2022, 7:57:13 PM
Evidence : 7300d >= 60mo			
2.192.0.92	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 7:33:33 PM
Evidence : 18250d >= 60mo			
2.192.0.56	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912		3/10/2022, 7:27:22 PM
Evidence : 7305d >= 60mo			
2.192.0.29	995b3eedc0b73b2fd244a7dded51dbabfe1c22f1bc5a24b87cf9fa45aab2a46e7	1	3/10/2022, 7:22:56 PM
Evidence : 7300d1h32m1s >= 825d			
2.192.8.23	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		3/10/2022, 6:37:48 PM
Evidence : 730d >= 398d			
2.192.3.216	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d		3/10/2022, 4:43:15 PM
Evidence : 7300d >= 60mo			
2.192.3.195	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 4:41:11 PM
Evidence : 9999d >= 60mo			
2.192.3.58	9de9742ccfca0b23118ed04d0f8c436cfbe1ada31fb91ffbed0befd862afe1c8c	1	3/10/2022, 4:37:17 PM
Evidence : 730d >= 398d			
2.192.10.39	c415794f859abcb944bc8a7b168967a5963a0179d5d4b2d25dabf242dc7ffe03	1	3/10/2022, 4:04:36 PM
Evidence : 3680d >= 825d			
2.192.3.112	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 3:56:39 PM
Evidence : 18250d >= 60mo			
2.192.1.141	bb826cd36f3b6f01458e391802a7068b3716f4c214de14760c95670f951abe53	1	3/10/2022, 11:37:01 AM
Evidence : 730d >= 398d			
2.192.11.136	983033524ba5518ed3f22df894c80b06d14d792dffe3b275495d6e9a5ce76cf9c	1	3/10/2022, 7:29:28 AM
Evidence : 730d >= 398d			
2.192.11.209	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		3/10/2022, 7:20:47 AM
Evidence : 730d >= 398d			
2.192.11.21	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 7:14:51 AM
Evidence : 9999d >= 60mo			
2.192.7.68	3d42db219fb46a96b8223836774b054f5514a5f5daded827e5c63bb5641793f4c		3/10/2022, 6:54:51 AM
Evidence : 730d >= 398d			
2.192.7.247	bd503c3b956fd2f76fd80b8e11100909b064dcb30f629e3e6b06c997416b862b	1	3/10/2022, 6:47:41 AM
Evidence : 730d >= 398d			
2.192.7.62	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912		3/10/2022, 6:37:23 AM
Evidence : 7305d >= 60mo			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.10.171	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		3/10/2022, 6:34:21 AM
Evidence : 730d >= 398d			
2.192.10.65	dee7de7afac7a23fe1624fb3670f5c25a4101268b7643dc0326466 1f80d687484		3/10/2022, 6:17:09 AM
Evidence : 730d >= 398d			
2.192.11.223	bf1ca590b3cc538370ee30d21debd52f7f513e3057a15b14d511f0532899c9a2a		3/10/2022, 6:16:39 AM
Evidence : 7300d >= 398d			
2.192.11.111	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/10/2022, 6:15:47 AM
Evidence : 9999d >= 60mo			
2.192.2.0	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d		3/10/2022, 5:56:59 AM
Evidence : 7300d >= 60mo			
2.192.6.165	47afbbb22314b00901c4524b601ae8d5871975ce5739cd4316612d95ddaa9646f	1	3/10/2022, 4:38:09 AM
Evidence : 18250d >= 60mo			
2.192.5.79	2b88cd6a6862e630db53858fd905a1911fc8ba1139ceddc11cce0bc7394c2e83	1	3/10/2022, 4:20:25 AM
Evidence : 6254d >= 398d			
2.192.5.239	ef1fd069e6f4fa81e139cb39d0bb049cca48e49808a04193e4674667089d1343	1	3/10/2022, 3:58:57 AM
Evidence : 3650d >= 60mo			
2.192.5.158	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/10/2022, 3:53:36 AM
Evidence : 7305d >= 60mo			
2.192.5.199	6be36afe45749ce202b1d2ba52e9dd30e14e2dafdf4872b391650d18fe20fd7e0	1	3/10/2022, 3:39:54 AM
Evidence : 3650d >= 60mo			
2.192.2.118	e002709f07e7e9e40342e6c26909092e1cfd6cd9f3b3d032da6e20e0ee89cadce	1	3/9/2022, 9:10:26 PM
Evidence : 9999d >= 60mo			
2.192.2.84	f29873c163f46c21d383ab714ae615fc55b5 1d4c0f85f966120471888e33afcc1	1	3/9/2022, 8:55:28 PM
Evidence : 1095d >= 398d			
2.192.2.171	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912		3/9/2022, 8:54:18 PM
Evidence : 7305d >= 60mo			
2.192.4.141	49a9d29d80d87b8ecc3a7874585d07f3953cf9d0dfd465169eaa87abcacd9dee	1	3/9/2022, 6:59:45 PM
Evidence : 730d >= 398d			
2.192.4.253	b26beb56f515052d6a9e7db1f34d24c7b9 1dba533c54adc60782dcb2682e27566	1	3/9/2022, 6:49:32 PM
Evidence : 7305d >= 60mo			
2.192.1.4	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		3/9/2022, 5:50:43 AM
Evidence : 730d >= 398d			
2.192.0.133	47afbbb22314b00901c4524b601ae8d5871975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 5:46:21 AM
Evidence : 18250d >= 60mo			
2.192.0.200	0eab86098cbc361b52a1280144d07c4a5515880700c98a18d0679571e795468a7		3/9/2022, 5:43:56 AM
Evidence : 7600d >= 398d			
2.192.0.189	0f3a7e2632f01e451aa855139f108ef65fc8 1c1d6128cd7d84cea0436cbab8d81	1	3/9/2022, 5:41:40 AM
Evidence : 730d >= 398d			
2.192.0.211	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		3/9/2022, 5:28:35 AM
Evidence : 730d >= 398d			
2.192.6.55	47afbbb22314b00901c4524b601ae8d5871975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 2:02:00 AM
Evidence : 18250d >= 60mo			
2.192.6.242	47afbbb22314b00901c4524b601ae8d5871975ce5739cd4316612d95ddaa9646f	1	3/9/2022, 1:48:02 AM
Evidence : 18250d >= 60mo			
2.192.7.7	1d6b73c5b8c91774e7a2a993759d71ebd1846c0fb6234f5a167e574eadd40312	1	3/9/2022, 1:43:46 AM
Evidence : 145983d1h41m45s >= 60mo			
2.192.6.54	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/9/2022, 1:37:35 AM
Evidence : 7305d >= 60mo			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.9.143	cc4a8a5280beac5f97de1fc9a8be98ad1781e3f1e7887accf7ad1239ef919729	1	3/8/2022, 6:59:13 PM
Evidence : 730d >= 398d			
2.192.4.164	b1b10ab845619a6cd7043a5f651dd3c9ac44f04e4041d9ba17d8a948ace14f2f	1	3/8/2022, 6:51:10 PM
Evidence : 7600d >= 825d			
2.192.9.125	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:48:03 PM
Evidence : 7305d >= 60mo			
2.192.4.34	7905ac7ab222693a18abc2bad129e1dc9198f5ec61faf3f82c64e3d6becaac1d	1	3/8/2022, 6:47:24 PM
Evidence : 3650d >= 60mo			
2.192.9.126	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:46:48 PM
Evidence : 7305d >= 60mo			
2.192.9.199	e45500a6cb74a7dc30628d79e4ec4ba9fa7dd0fe404b270b249e766a61d6ac82	1	3/8/2022, 6:45:50 PM
Evidence : 3650d >= 398d			
2.192.4.48	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:45:11 PM
Evidence : 18250d >= 60mo			
2.192.10.6	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	3/8/2022, 6:34:25 PM
Evidence : 18250d >= 60mo			
2.192.4.41	94eaa1c54a054b484868342bd9e6d6ec5256e4ef2ec655b2063e438d814cb191	1	3/8/2022, 6:34:21 PM
Evidence : 730d >= 398d			
2.192.9.112	743f6840b846750b764eb65a556ae1e2b83862ab59ee0e5388e06a9c0f3297f2	1	3/8/2022, 6:05:08 PM
Evidence : 3680d >= 398d			
2.192.0.202	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	3/6/2022, 12:19:31 AM
Evidence : 730d >= 398d			
2.192.11.17	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	2/24/2022, 9:48:40 PM
Evidence : 7300d >= 60mo			
2.192.7.50	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d	1	2/23/2022, 12:58:43 AM
Evidence : 730d >= 398d			
2.192.6.117	d0616a7224a8f6d34a4c1c4fc1e5398183e3069674a8b64f78204cb41eb1b879	1	2/20/2022, 10:54:17 PM
Evidence : 6259d >= 398d			
2.192.4.117	974a16997ca42b9731f50d2d727fa6bca70190c865357b0003b52a0bd307c4a8	1	2/18/2022, 3:51:33 PM
Evidence : 6160d >= 398d			
2.192.0.37	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/18/2022, 8:24:46 AM
Evidence : 18250d >= 60mo			
2.192.1.157	4e31dfe1eb03f38e7122e2702937911a12cbd67f556ae3351f58d43d8cf02e96	1	2/18/2022, 8:02:56 AM
Evidence : 3680d >= 398d			
2.192.5.164	75eb15acbf13d4c39766110f766d2cb0369034603ddc2548b4d284d30243f0cd	1	2/18/2022, 6:53:52 AM
Evidence : 730d >= 398d			
2.192.11.5	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 1:07:54 PM
Evidence : 18250d >= 60mo			
2.192.10.229	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 1:05:41 PM
Evidence : 18250d >= 60mo			
2.192.4.228	4fec42fbb2a17a39e02c9a03e24d5e7a54e715b964cfb2fd8231367ea4a7fade	1	2/15/2022, 10:31:41 AM
Evidence : 7300d >= 39mo			
2.192.6.143	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 10:04:50 AM
Evidence : 18250d >= 60mo			
2.192.9.145	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/15/2022, 9:28:06 AM
Evidence : 18250d >= 60mo			
2.192.0.44	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	2	2/15/2022, 9:19:40 AM
Evidence : 18250d >= 60mo			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.4.109	47afbbb22314b00901c4524b601ae8d587 1 975ce5739cd4316612d95ddaa9646f		2/15/2022, 6:47:55 AM
Evidence : 18250d >= 60mo			
2.192.8.94	c4a148013f7b023b84b003e316626c52cb 1 e5ea128a378beabb1a19254073ff2d		2/15/2022, 2:19:50 AM
Evidence : 22080d >= 39mo			
2.192.11.151	dee7de7afac7a23fe1624fb3670f5c25a4102 268b7643dc03264661f80d687484		2/12/2022, 4:56:25 AM
Evidence : 730d >= 398d			
2.192.10.36	9de9742ccfca0b23118ed04d0f8c436cfbe1 ada31fb91ffbed0befd862afe1c8c		2/11/2022, 10:33:43 AM
Evidence : 730d >= 398d			
2.192.5.162	7905ac7ab222693a18abc2bad129e1dc9191 8f5ec61faf3f82c64e3d6becaac1d		2/11/2022, 10:05:12 AM
Evidence : 3650d >= 60mo			
2.192.6.252	ec0b77d7cb90e1f175b7fbf332cf331ff11cd61 0b4f894dbed128f8db7a052bbe		2/11/2022, 6:34:02 AM
Evidence : 10951d >= 398d			
2.192.6.243	3fea6e1fdc8aeac6463615badb58eaccc4c 1 c2b092e27bdd1693adf1250189741		2/11/2022, 6:23:37 AM
Evidence : 730d >= 398d			
2.192.11.69	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		2/11/2022, 12:16:45 AM
Evidence : 7305d >= 60mo			
2.192.3.121	bbecca6f745bc239331bd4b3cee07493d51 04ee0965a055a04f487fc9141baf6d		2/10/2022, 11:05:03 PM
Evidence : 730d >= 398d			
2.192.3.100	85eb21e49e9d8b2797747dffde96ba0123 1 6bd9c14e6b0ae1e6c7b544c706bf44		2/10/2022, 11:01:28 PM
Evidence : 1095d >= 825d			
2.192.3.135	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		2/10/2022, 11:01:16 PM
Evidence : 7305d >= 60mo			
2.192.3.59	47afbbb22314b00901c4524b601ae8d587 1 975ce5739cd4316612d95ddaa9646f		2/10/2022, 10:56:12 PM
Evidence : 18250d >= 60mo			
2.192.0.155	00cf2c6fdad819da6310cbd9b5a53ea5c3 1 7366dcc2c529f3683203f8bcf09cca		2/10/2022, 8:02:02 PM
Evidence : 3650d >= 825d			
2.192.0.79	49a9d29d80d87b8ecc3a7874585d07f39 1 53cf9d0dfd465169eaa87abcacd9dee		2/10/2022, 7:54:03 PM
Evidence : 730d >= 398d			
2.192.10.73	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		2/10/2022, 7:47:50 PM
Evidence : 7305d >= 60mo			
2.192.4.221	ff67e5f5e2609307f04dd9bc000cfcf0ca41 594d7e0acd7912f458e96a380504d		2/10/2022, 12:42:26 PM
Evidence : 7300d >= 60mo			
2.192.6.3	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		2/10/2022, 6:39:53 AM
Evidence : 9999d >= 60mo			
2.192.6.210	9de9742ccfca0b23118ed04d0f8c436cfbe1 ada31fb91ffbed0befd862afe1c8c		2/10/2022, 3:50:28 AM
Evidence : 730d >= 398d			
2.192.11.49	995b3eedc0b73b2fd244a7dded51dbabfe1 c22f1bc5a24b87cf9fa45aab2a46e7		2/10/2022, 2:08:51 AM
Evidence : 7300d1h32m1s >= 825d			
2.192.7.50	56081d5a3fb79ee327cbc6843a6f217db17 1 b697535e41f3397d9380433fd7973		2/9/2022, 10:12:20 PM
Evidence : 3650d >= 825d			
2.192.7.231	83a34fab143a111a251c9335f78b2cc74dfdc1 46e9b1d124487e2f4942187db9b		2/9/2022, 10:09:21 PM
Evidence : 3680d >= 398d			
2.192.7.96	47afbbb22314b00901c4524b601ae8d587 1 975ce5739cd4316612d95ddaa9646f		2/9/2022, 10:07:21 PM
Evidence : 18250d >= 60mo			
2.192.7.146	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		2/9/2022, 10:05:32 PM
Evidence : 7305d >= 60mo			
2.192.11.83	dee7de7afac7a23fe1624fb3670f5c25a4101 268b7643dc03264661f80d687484		2/9/2022, 9:41:54 PM
Evidence : 730d >= 398d			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.11.56	cc4a8a5280beac5f97de1fc9a8be98ad1781e3f1e7887accf7ad1239ef919729	1	2/9/2022, 9:41:51 PM
Evidence : 730d >= 398d			
2.192.11.203	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/9/2022, 9:38:49 PM
Evidence : 9999d >= 60mo			
2.192.11.167	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 9:25:09 PM
Evidence : 18250d >= 60mo			
2.192.9.222	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/9/2022, 12:26:57 AM
Evidence : 18250d >= 60mo			
2.192.1.155	f18993e590db02cb92dc63335bd5fb96d40e5b68dd4bdc5dfa148959a0af356f	1	2/8/2022, 10:08:50 PM
Evidence : 730d >= 398d			
2.192.1.162	30dd8cba5ababe04616399e56e9f7b46af5c9ab3fca5300e97bf84b80fcf5e14	1	2/8/2022, 10:08:27 PM
Evidence : 1095d >= 825d			
2.192.1.19	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:05:21 PM
Evidence : 18250d >= 60mo			
2.192.1.207	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 10:04:11 PM
Evidence : 18250d >= 60mo			
2.192.1.214	bbecca6f745bc239331bd4b3cee07493d5104ee0965a055a04f487fc9141baf6d		2/8/2022, 9:51:37 PM
Evidence : 730d >= 398d			
2.192.1.53	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/8/2022, 9:51:35 PM
Evidence : 9999d >= 60mo			
2.192.4.159	d12345b3395500b077e84dd001866f7f6a102cd862d4d38d62e380988d57a15b0	1	2/8/2022, 9:43:48 PM
Evidence : 1095d >= 825d			
2.192.4.43	47afbbb22314b00901c4524b601ae8d587975ce5739cd4316612d95ddaa9646f	1	2/8/2022, 9:42:30 PM
Evidence : 18250d >= 60mo			
2.192.4.215	0f514f8672d55cb9edefca40e9925d9fc36102b4ef5dcdcbb2a9c955eeadaa0e1		2/8/2022, 9:40:53 PM
Evidence : 730d >= 398d			
2.192.0.43	ef72b5f1a1ac614a1e2c83b8a65201d87bcabe4ef16db340eb8705e709ae986e	1	2/8/2022, 8:39:59 PM
Evidence : 3650d >= 825d			
2.192.0.90	380fae1b309686b9703cd35fd31d75010f5187d4222c87f78da7e8c8053cbbf3c		2/8/2022, 8:28:58 PM
Evidence : 3650d >= 398d			
2.192.8.230	b1b10ab845619a6cd7043a5f651dd3c9ac44f04e4041d9ba17d8a948ace14f2f	1	2/8/2022, 6:54:10 PM
Evidence : 7600d >= 825d			
2.192.9.145	94eaa1c54a054b484868342bd9e6d6ec5256e4ef2ec655b2063e438d814cb191	1	2/8/2022, 5:24:56 AM
Evidence : 730d >= 398d			
2.192.7.250	c9c98101f12f59134432c49ce306305c9314f941c9e9d3af1bca44bb7dc64cd8	1	2/7/2022, 5:01:21 AM
Evidence : 1095d >= 825d			

Certificate Signed With Weak Algorithm

A certificate was observed that was signed with a weak algorithm.

-1.2 SCORE IMPACT

Description

When a Certificate Authority (CA) issues a certificate, it is signed with one of the defined algorithms supported expected to be supported by TLS clients (e.g., web browser). Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. Consensus on which algorithms are untrustworthy evolves over time, and if a certificate is signed with a weak algorithm then that certificate can be altered or faked.

Recommendation

If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.

59 findings

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.1.171	98b4742f431440761c7fd201eec206c44661 3ca0b3beee347d56f04cf792e89f4		3/11/2022, 7:16:49 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.1.106	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/11/2022, 7:03:20 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.192	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/11/2022, 1:31:43 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.247	ff67e5f5e2609307f04dd9bc000cfcf0ca41 594d7e0acd7912f458e96a380504d		3/10/2022, 7:57:13 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.159	1e33fae1dfa19928f1d739b821ff9f14c5bc98 1 5fe746e20f1510a1eea3d8ed7b		3/10/2022, 7:36:06 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.0.56	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		3/10/2022, 7:27:22 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.3.216	ff67e5f5e2609307f04dd9bc000cfcf0ca41 594d7e0acd7912f458e96a380504d		3/10/2022, 4:43:15 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.3.195	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/10/2022, 4:41:11 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.11.21	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/10/2022, 7:14:51 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.62	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		3/10/2022, 6:37:23 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.11.229	6158658b038a8ad15445d27c44c2c7282a1 bb609d5f5a978b7970fb37bb6a61a2		3/10/2022, 6:26:17 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.11.111	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/10/2022, 6:15:47 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.0	ff67e5f5e2609307f04dd9bc000cfcf0ca41 594d7e0acd7912f458e96a380504d		3/10/2022, 5:56:59 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.5.158	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		3/10/2022, 3:53:36 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.5.199	6be36afe45749ce202b1d2ba52e9dd30e 1 4e2dafdf4872b391650d18fe20fd7e0		3/10/2022, 3:39:54 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.118	e002709f07e7e9e40342e6c26909092e 1 cfd6cd9f3b3d032da6e20e0ee89cadce		3/9/2022, 9:10:26 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.18	8a6511e0835f5bbd71a34a273c91d5cabd3 1 0af2a79e3b88a103a6f61c34691d0		3/9/2022, 8:55:31 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.84	f29873c163f46c21d383ab714ae615fc55b5 1 d4c0f85f966120471888e33afcc1		3/9/2022, 8:55:28 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.171	ff0cb6ffc548545a43bd3f284a333a96d4ff1 1c23ebd09771b3928ff749b08912		3/9/2022, 8:54:18 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.2.175	a9ddd4aa8b5c6049d87b2654e2326244 1 4f91befda60c7a4c3d8bc8ed6aff417b		3/9/2022, 8:51:05 PM
Evidence : md5_rsa (1.2.840.113549.1.1.4)			
2.192.4.253	b26beb56f515052d6a9e7db1f34d24c7b9 1 dba533c54adc60782dcb2682e27566		3/9/2022, 6:49:32 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.148	98b4742f431440761c7fd201eec206c44661 3ca0b3beee347d56f04cf792e89f4		3/9/2022, 4:23:34 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.6.23	c7fd6d5d51e06ba71fea12d27f8e646b1d7f 1 ecd845c5d50f584949b0fa58dfd3		3/9/2022, 1:51:10 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.7	1d6b73c5b8c91774e7a2a993759d71ebd18 1 46c0fb6234f5a167e574eadd40312		3/9/2022, 1:43:46 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.6.218	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/9/2022, 1:37:44 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.6.54	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/9/2022, 1:37:35 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.125	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:48:03 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.4.34	7905ac7ab222693a18abc2bad129e1dc91918f5ec61faf3f82c64e3d6becaac1d	1	3/8/2022, 6:47:24 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.126	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	3/8/2022, 6:46:48 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.144	98b4742f431440761c7fd201eec206c4466133ca0b3beee347d56f04cf792e89f4	1	3/8/2022, 6:11:38 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.104	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	3/8/2022, 6:11:35 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.5.162	7905ac7ab222693a18abc2bad129e1dc91918f5ec61faf3f82c64e3d6becaac1d	1	2/11/2022, 10:05:12 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.4.237	af10a28e8fc466dc62a2aa6247ec5b1daec18b77e9cf0bb5ecf54ecc57da91fee	1	2/11/2022, 9:56:44 AM
Evidence : md5_rsa (1.2.840.113549.1.1.4)			
2.192.5.182	a9ddd4aa8b5c6049d87b2654e232624414f91befda60c7a4c3d8bc8ed6aff417b	1	2/11/2022, 9:51:02 AM
Evidence : md5_rsa (1.2.840.113549.1.1.4)			
2.192.6.118	728a52efa109420a1c892041e9637280e43b3d7f4547435e24bab02b6cd3aff6	1	2/11/2022, 6:23:45 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.11.69	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/11/2022, 12:16:45 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.3.232	8c4129a0634eba1a1d341815ef59f64b6a5c1d03ad0ede85e9f31e29545dce082	1	2/10/2022, 11:02:29 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.3.142	2c4ff0142914b45174c478d1ac5347279eb15edbb2dc37d6fe180b6511fe989c8	1	2/10/2022, 11:02:18 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.3.135	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 11:01:16 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.0.38	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 8:13:33 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.0.100	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/10/2022, 8:02:09 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.10.64	547ff655f1ef78800409f359730bc20f737e3a566e8eabb3a0106586c100aca2	1	2/10/2022, 7:53:51 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.10.73	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/10/2022, 7:47:50 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.4.221	ff67e5f5e2609307f04dd9bc000cfcf0ca41594d7e0acd7912f458e96a380504d	1	2/10/2022, 12:42:26 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.5.250	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 6:45:29 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.6.3	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/10/2022, 6:39:53 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.6.100	98b4742f431440761c7fd201eec206c4466133ca0b3beee347d56f04cf792e89f4	1	2/10/2022, 3:42:39 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.6.26	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:52 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.6.176	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:37 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.66	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 10:09:46 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.146	ff0cb6ffc548545a43bd3f284a333a96d4ff11c23ebd09771b3928ff749b08912	1	2/9/2022, 10:05:32 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.11.203	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/9/2022, 9:38:49 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.26	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/9/2022, 7:27:05 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.10.212	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 4:10:30 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.7.25	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	2/9/2022, 9:20:17 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.9.177	1e33fae1dfa19928f1d739b821ff9f14c5bc9815fe746e20f1510a1eea3d8ed7b	1	2/9/2022, 12:21:47 AM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.1.53	e002709f07e7e9e40342e6c26909092ecfd6cd9f3b3d032da6e20e0ee89cadce	1	2/8/2022, 9:51:35 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.8.65	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/8/2022, 6:56:34 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			
2.192.8.175	b37d66a37f48fbdd7949e48442836393dcc10f9511507f663a8d4fc59b48cb79	1	2/8/2022, 6:48:07 PM
Evidence : sha1withrsaencryption (1.2.840.113549.1.1.5)			

DNS Server Accessible

We discovered a DNS server running on your network perimeter, accessible to the internet.

Description

It is not inherently risky to expose a DNS server, which translates domain names, such as example.com, into IP addresses that browsers use to find and access web sites. Most network operators aid public web navigation with internet-facing DNS servers. A misconfigured DNS server, however, can be vulnerable to a malicious redirection of web R or a distributed denial of service (DDoS) attack, where an attacker floods a domain's DNS servers to disrupt DNS resolution for that domain.

Recommendation

Perform a security audit of your DNS server configuration and apply any necessary controls, such as a firewall or DNS Security Extensions.

2 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
DNS Server	2.192.0.131	53	2/18/2022, 11:49:43 AM
DNS Server	2.192.0.161	53	2/7/2022, 11:46:31 AM

SSH Supports Weak MAC

-0.3 SCORE IMPACT

A weak Message Authentication Code (MAC) algorithm has been detected.

Description

Recommendation

The SSH server is configured to support MD5 algorithm. The cryptographic strength depends upon the size of the key and algorithm that is used. A Modern MAC algorithms such as SHA1 or SHA2 should be used instead.

Configure the SSH server to disable the use of MD5.

1 finding

IP ADDRESS	PORT	LAST OBSERVED
2.192.7.28	22	2/24/2022, 2:51:28 PM
Evidence : hmac-sha1-96		

RDP Service Observed

-0.3 SCORE IMPACT

We observed RDP, a remote access service, publicly exposed.

Description
The RDP protocol offers remote access to a host, providing a view of the host's console as output and accepting keyboard and mouse events as input.
We observed an RDP service on the Internet, accessible by the public. Remote access services are attractive targets to attackers because they provide remote control over a host. Once logged-in, users can install programs, access files, and run commands on the host. Attackers can add hosts over which they have gained control to botnets, adding the host's computational capabilities and bandwidth to their spam, malware, or distributed denial-of-service (DDoS) campaigns. Attackers may target the service with authentication bypass attacks (e.g., brute-forcing, buffer overflows, blank passwords) in an attempt to gain control of the host or exfiltrate its databases. Due to sharing user authentication databases with other Microsoft services, brute-forcing this service may provide credentials useful on other services. Attackers may launch denial-of-service (DoS) attacks against the service, rendering the service unusable by authorized entities. A compromised host may allow an attacker to penetrate further into the host's associated infrastructure.

Recommendation
Exposing remote access services to the Internet is not recommended. Consider placing the service behind a VPN, preventing public access. If making the service private is not possible, restrict the service by allowlisting the IP addresses that require access.

1 finding

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Microsoft Terminal Services	2.192.9.120	3389	2/7/2022, 12:52:38 PM

Certificate Is Expired

-1.4 SCORE IMPACT

Expired certificates prevent TLS clients from connecting to servers.

Description
When a Certificate Authority (CA) issues a certificate, they embed two dates: the date at which the certificate starts being valid, and the date at which the certificate stops being valid. If a TLS client (e.g., web browser) connects to a TLS server (e.g., website) and receives a certificate that is expired, then the TLS client will refuse to connect.
Certificates are digital assets that require renewal or decommissioning on a schedule.

Recommendation
Services presenting expired certificates should cause noticeable failures, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact the CA and arrange issuance of a new certificate.
Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

64 findings

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.1.99	495e762b5aa7fd9dd83c3947f94f0d91f0fd0a2722b346f07f2038ea4525f5f3	1	3/11/2022, 7:20:14 AM
Evidence : Mon Dec 13 2021 00:58:29 GMT+0000 (Coordinated Universal Time)			
2.192.1.171	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/11/2022, 7:16:49 AM
Evidence : Sat Jan 27 2018 13:14:54 GMT+0000 (Coordinated Universal Time)			
2.192.1.149	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/11/2022, 7:03:49 AM
Evidence : Sat Feb 26 2022 21:26:46 GMT+0000 (Coordinated Universal Time)			
2.192.1.60	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	3/11/2022, 6:55:28 AM
Evidence : Wed Jun 03 2020 13:12:31 GMT+0000 (Coordinated Universal Time)			
2.192.2.159	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/10/2022, 7:36:06 PM
Evidence : Fri Jan 15 2016 14:54:51 GMT+0000 (Coordinated Universal Time)			
2.192.8.234	57ef50936a84664f41134c375c372c61917e1a9480436eeb19eb8ea074b43503	1	3/10/2022, 6:34:54 PM
Evidence : Sun Jul 11 2021 10:13:26 GMT+0000 (Coordinated Universal Time)			
2.192.10.86	a6951a61b0adf3e54897349d17de9f0c3701f20012eee9a7170b1aaddf8e89b79	1	3/10/2022, 7:25:56 AM
Evidence : Wed Jun 03 2020 13:12:43 GMT+0000 (Coordinated Universal Time)			
2.192.11.62	ee5e83ea61be05e0b8ef9782344d809abd1aabad10ac1019bf3aeaaa9a98d9af	1	3/10/2022, 7:25:29 AM
Evidence : Sun May 30 2021 10:51:00 GMT+0000 (Coordinated Universal Time)			
2.192.11.106	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	3/10/2022, 7:15:35 AM
Evidence : Thu Nov 25 2021 09:47:35 GMT+0000 (Coordinated Universal Time)			
2.192.10.53	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 6:31:04 AM
Evidence : Sat Feb 26 2022 21:26:46 GMT+0000 (Coordinated Universal Time)			
2.192.11.229	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	3/10/2022, 6:26:17 AM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.6.13	6831970d31c8b170ab443da794bc84da273f3a120ae76fddbed757a1d7db63b5	1	3/10/2022, 3:55:12 AM
Evidence : Sat Feb 26 2022 21:26:46 GMT+0000 (Coordinated Universal Time)			
2.192.5.166	1036a96b07223f3ac421e92f3f3f1221ee8998ff875c1e3448c870bbb6d881f2	1	3/10/2022, 3:46:45 AM
Evidence : Sat Feb 26 2022 21:26:28 GMT+0000 (Coordinated Universal Time)			
2.192.2.18	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	3/9/2022, 8:55:31 PM
Evidence : Thu Mar 14 2019 09:56:25 GMT+0000 (Coordinated Universal Time)			
2.192.0.234	be8aaaad93b39f9007a5ac6fadf236616f3d38b3dbba258b36bc2d2c80703e01	1	3/9/2022, 5:47:27 AM
Evidence : Wed Jun 03 2020 13:13:01 GMT+0000 (Coordinated Universal Time)			
2.192.0.206	01ea22c3220f4e8ee3a9b7d0eb088c4c8b43a360a837eb4f4524d833342ae8dd	1	3/9/2022, 5:46:16 AM
Evidence : Fri Mar 06 2020 23:59:59 GMT+0000 (Coordinated Universal Time)			
2.192.7.148	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/9/2022, 4:23:34 AM
Evidence : Sat Jan 27 2018 13:14:54 GMT+0000 (Coordinated Universal Time)			
2.192.6.23	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	3/9/2022, 1:51:10 AM
Evidence : Wed Oct 19 2011 09:25:32 GMT+0000 (Coordinated Universal Time)			
2.192.6.218	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	3/9/2022, 1:37:44 AM
Evidence : Fri Jan 15 2016 14:54:51 GMT+0000 (Coordinated Universal Time)			
2.192.5.168	01ea22c3220f4e8ee3a9b7d0eb088c4c8b43a360a837eb4f4524d833342ae8dd	1	3/9/2022, 1:09:42 AM
Evidence : Fri Mar 06 2020 23:59:59 GMT+0000 (Coordinated Universal Time)			
2.192.5.128	d8664eaf6fba634791ff6d3b9ae26c0d6c21a4a5ac54868d58a243358ed12737a	1	3/9/2022, 12:55:57 AM
Evidence : Thu Nov 25 2021 09:47:50 GMT+0000 (Coordinated Universal Time)			
2.192.9.236	15e291ef2b9d8a5316714c3a48898e9abfb207bd90fb287d3ef2dab747183daa3	2	3/8/2022, 6:49:22 PM
Evidence : Wed Mar 17 2021 12:47:26 GMT+0000 (Coordinated Universal Time)			
2.192.9.144	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4	1	3/8/2022, 6:11:38 PM
Evidence : Sat Jan 27 2018 13:14:54 GMT+0000 (Coordinated Universal Time)			
2.192.9.104	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	3/8/2022, 6:11:35 PM
Evidence : Thu Mar 14 2019 09:56:25 GMT+0000 (Coordinated Universal Time)			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.5.9	0bdaee6af1262fef5d0f03dd02f7efcd540974e0b6bf6d2ef8a5167213560474	1	2/23/2022, 10:19:49 PM
Evidence : Sat Jan 05 2013 08:02:14 GMT+0000 (Coordinated Universal Time)			
2.192.5.162	5ddcd1559efb72079b654485c66c18acafe134606b9bda30b2fbe9cb44fa455c6	1	2/22/2022, 3:13:55 AM
Evidence : Thu May 07 2020 06:52:13 GMT+0000 (Coordinated Universal Time)			
2.192.9.144	13dcd3ff251061088dfe72eb30069786773159022d9a90d1a2d30655e1ad24382	1	2/15/2022, 9:28:05 AM
Evidence : Wed Nov 18 2020 18:07:36 GMT+0000 (Coordinated Universal Time)			
2.192.5.172	6f503ea0843c3228b3704cce7c4c6f1e3e14421ed960ce8260506c959bd841e86	1	2/11/2022, 10:00:41 AM
Evidence : Sun Jul 11 2021 10:13:35 GMT+0000 (Coordinated Universal Time)			
2.192.5.58	80e089dd74979ae84d9a2e1b45c698726adafcec4c6ca183b9f3f7f0cdb2e542	1	2/11/2022, 9:55:34 AM
Evidence : Thu Dec 10 2020 07:38:51 GMT+0000 (Coordinated Universal Time)			
2.192.4.185	7f621bb6fa2ad11096c354dad397b3d6fc711737fee400c0f3a92d3bf991f6403	1	2/11/2022, 9:48:04 AM
Evidence : Sun Nov 03 2019 09:44:01 GMT+0000 (Coordinated Universal Time)			
2.192.2.174	c80b2e6bf2c33cd85bbb2220a301f3ccc0101e43355de8cff04b1274eb6f85414	1	2/11/2022, 9:39:12 AM
Evidence : Tue Aug 10 2021 14:47:23 GMT+0000 (Coordinated Universal Time)			
2.192.6.118	728a52efa109420a1c892041e9637280e43b3d7f4547435e24bab02b6cd3aff6	1	2/11/2022, 6:23:45 AM
Evidence : Wed Jan 01 2020 03:21:15 GMT+0000 (Coordinated Universal Time)			
2.192.3.159	1172d82213af66fba30f80af18572648b2d38b524e238206bde88a131892ea78	1	2/10/2022, 11:09:44 PM
Evidence : Sat Mar 06 2021 13:49:29 GMT+0000 (Coordinated Universal Time)			
2.192.3.75	27d8bf86ebc677f9455c823cecab4c800ac32f47abacac38962cfc04417525be	2	2/10/2022, 11:02:42 PM
Evidence : Fri Nov 12 2021 12:41:32 GMT+0000 (Coordinated Universal Time)			
2.192.3.232	8c4129a0634eba1a1d341815ef59f64b6a5c1d03ad0ede85e9f31e29545dce082	1	2/10/2022, 11:02:29 PM
Evidence : Fri Jan 15 2016 14:54:48 GMT+0000 (Coordinated Universal Time)			
2.192.3.142	2c4ff0142914b45174c478d1ac5347279eb15edbb2dc37d6fe180b6511fe989c8	1	2/10/2022, 11:02:18 PM
Evidence : Sun Jun 25 2017 12:03:49 GMT+0000 (Coordinated Universal Time)			
2.192.0.38	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 8:13:33 PM
Evidence : Thu Mar 14 2019 09:56:25 GMT+0000 (Coordinated Universal Time)			
2.192.0.250	330ce1b1ff663370f80f3187a90186b844521296e286de9fc407bc0d98dd35be9	1	2/10/2022, 8:03:45 PM
Evidence : Wed Jun 03 2020 13:12:31 GMT+0000 (Coordinated Universal Time)			
2.192.0.100	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/10/2022, 8:02:09 PM
Evidence : Wed Oct 19 2011 09:25:32 GMT+0000 (Coordinated Universal Time)			
2.192.10.64	547ff655f1ef78800409f359730bc20f737e3a566e8eabb3a0106586c100aca2	1	2/10/2022, 7:53:51 PM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.5.250	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/10/2022, 6:45:29 AM
Evidence : Thu Mar 14 2019 09:56:25 GMT+0000 (Coordinated Universal Time)			
2.192.6.100	98b4742f431440761c7fd201eec206c4466113ca0b3beee347d56f04cf792e89f4	1	2/10/2022, 3:42:39 AM
Evidence : Sat Jan 27 2018 13:14:54 GMT+0000 (Coordinated Universal Time)			
2.192.6.26	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:52 AM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.6.176	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/10/2022, 3:35:37 AM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.7.117	b1daa07922bdca09ed41c7c595bebfcb800d22452fdf7f40a46a99d1289d1b36	1	2/9/2022, 10:14:26 PM
Evidence : Wed Aug 25 2021 05:30:56 GMT+0000 (Coordinated Universal Time)			
2.192.7.66	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 10:09:46 PM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.7.42	57bd0384a64c64f63b986d5d82162cba311acc045ef9af0dcf1f13f5d8b6fef11	1	2/9/2022, 10:00:26 PM
Evidence : Wed Mar 17 2021 12:47:09 GMT+0000 (Coordinated Universal Time)			
2.192.7.116	d8664eaf6fba634791ff6d3b9ae26c0d6c21a4a5ac54868d58a243358ed12737a	1	2/9/2022, 9:59:01 PM
Evidence : Thu Nov 25 2021 09:47:50 GMT+0000 (Coordinated Universal Time)			

TARGET	SHA-256 FINGERPRINT	OBSERVATIONS	LAST OBSERVED
2.192.9.26	8a6511e0835f5bbd71a34a273c91d5cabd30af2a79e3b88a103a6f61c34691d0	1	2/9/2022, 7:27:05 PM
Evidence : Thu Mar 14 2019 09:56:25 GMT+0000 (Coordinated Universal Time)			
2.192.0.249	0b84d07fa94be76fc4a7b82a43a88b532b3d211031c10b8b49f3e40a5a507d4ae		2/9/2022, 4:55:42 PM
Evidence : Fri Jan 03 2020 13:51:48 GMT+0000 (Coordinated Universal Time)			
2.192.0.158	a3aa99d4c86db0b3f3bd7011e1ede7fcd109744e2fbbe6fb52bfdc94d3d3b055	1	2/9/2022, 4:43:04 PM
Evidence : Sun Nov 14 2021 11:43:19 GMT+0000 (Coordinated Universal Time)			
2.192.10.152	6ab09b14de3a32a30909a8c9e3ad7b3cd1487d208b9480c80ac01a8d86d60e476	1	2/9/2022, 4:19:19 PM
Evidence : Sun Nov 14 2021 11:43:23 GMT+0000 (Coordinated Universal Time)			
2.192.10.212	6158658b038a8ad15445d27c44c2c7282a1bb609d5f5a978b7970fb37bb6a61a2	1	2/9/2022, 4:10:30 PM
Evidence : Fri Jan 15 2016 14:54:49 GMT+0000 (Coordinated Universal Time)			
2.192.7.25	98b4742f431440761c7fd201eec206c446613ca0b3beee347d56f04cf792e89f4		2/9/2022, 9:20:17 AM
Evidence : Sat Jan 27 2018 13:14:54 GMT+0000 (Coordinated Universal Time)			
2.192.9.173	2ca23ad3a8a9ac5637054c6207db6d1f3b219b996f0dc47cfcca9c7847694cafa	2	2/9/2022, 12:40:31 AM
Evidence : Sun Jul 11 2021 10:14:37 GMT+0000 (Coordinated Universal Time)			
2.192.9.223	58e1488de43e5a4ed6872ff8961e61834cb17cb2315c305bed8d7eecf2cad0bb9	1	2/9/2022, 12:28:08 AM
Evidence : Thu Nov 25 2021 09:47:35 GMT+0000 (Coordinated Universal Time)			
2.192.9.177	1e33fae1dfa19928f1d739b821ff9f14c5bc985fe746e20f1510a1eea3d8ed7b	1	2/9/2022, 12:21:47 AM
Evidence : Fri Jan 15 2016 14:54:51 GMT+0000 (Coordinated Universal Time)			
2.192.1.168	943be5cb86129d95ace9a15080fde86e301c0588023a288ca94cf945b9dc8c8f	1	2/8/2022, 10:18:33 PM
Evidence : Fri May 29 2020 11:10:14 GMT+0000 (Coordinated Universal Time)			
2.192.1.172	9c34af632db9569f9222b22fecc85a3cdb10a535dcdf55d4a2ec8dd26dc9ad855	1	2/8/2022, 10:03:30 PM
Evidence : Wed Mar 17 2021 12:46:45 GMT+0000 (Coordinated Universal Time)			
2.192.4.228	ee5e83ea61be05e0b8ef9782344d809abd1aabad10ac1019bf3aeaaa9a98d9af	1	2/8/2022, 9:52:11 PM
Evidence : Sun May 30 2021 10:51:00 GMT+0000 (Coordinated Universal Time)			
2.192.9.254	a6951a61b0adf3e54897349d17de9f0c3701f20012eee9a7170b1aaddf8e89b79		2/8/2022, 8:21:48 PM
Evidence : Wed Jun 03 2020 13:12:43 GMT+0000 (Coordinated Universal Time)			
2.192.8.65	c7fd6d5d51e06ba71fea12d27f8e646b1d7fecd845c5d50f584949b0fa58dfd3	1	2/8/2022, 6:56:34 PM
Evidence : Wed Oct 19 2011 09:25:32 GMT+0000 (Coordinated Universal Time)			
2.192.8.175	b37d66a37f48fbdd7949e48442836393dcc10f9511507f663a8d4fc59b48cb79	1	2/8/2022, 6:48:07 PM
Evidence : Fri Jan 01 2021 00:00:54 GMT+0000 (Coordinated Universal Time)			
2.192.10.69	2847b80e41751d4d7b532e6259d1709d1535d1dd440a5a90a961b94d86d6fbbf	1	2/7/2022, 11:06:41 AM
Evidence : Thu Nov 25 2021 09:47:35 GMT+0000 (Coordinated Universal Time)			

PPTP Service Accessible

-0.3 SCORE IMPACT

We observed a service running PPTP, an obsolete and insecure VPN-like protocol, publicly exposed.

Description

The point-to-point tunneling protocol (PPTP) is an obsolete method for implementing virtual private networks (VPN). PPTP has well known security issues. It uses TCP and a tunnel protocol to encapsulate PPP packets. Many modern VPNs use various forms of user datagram protocol (UDP), which is a better alternative. Researchers have found that brute-forcing the encryption on PPTP connections is trivial. There are other issues with improper key size settings, making it easy for operators to improperly deploy PPTP. There are modern, more secure, and better alternatives for VPN implementations, such as OpenVPN, IPSec, IKEv2, and L2TP.

Recommendation

Review the business necessity of running a PPTP service on your network. PPTP is an obsolete and insecure method for implementing VPNs. Migrate the service to a more secure VPN implementation, such as OpenVPN.

1 finding

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Point-to-Point Tunnelling Protocol Service	2.192.3.159	1723	2/12/2022, 4:32:09 AM

UPnP Accessible

We observed publicly exposed UPnP-enabled devices.

Description
Universal Plug and Play (UPnP) protocols enable control of diverse networked devices, such as computers, printers, tablets,
mobile phones, internet gateways, and Wi-Fi access points. Using this protocol, devices discover each other and establish mutual working configurations.

While UPnP provides a lot of convenience, it is intended primarily for residential networks. As a business implementation,
it poses several security issues:
- The UPnP protocol, by default, does not implement authentication. This potentially leaves routers and firewalls running
the UPnP Internet Gateway Device Protocol (IGPD) vulnerable to attack.
- UPnP IGD devices that allow UPnP requests from the internet are also vulnerable to attack.
- A protocol design flaw named "CallStranger", found in billions of UPnP devices, enables an attacker to
- Exfiltrate data, even if you have proper data loss prevention or border security measures in place
- Scan your network
- Cause your network to participate in a DDoS attack

Recommendation
Review the business need of exposing UPnP-enabled devices. Hide them behind a firewall, or make them accessible only on an intranet.

2 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
UPNP Service	2.192.4.73	5000	2/8/2022, 12:33:32 PM
UPNP Service	2.192.5.76	5000	2/7/2022, 12:53:31 PM

SSH Software Supports Vulnerable Protocol

-0.7 SCORE IMPACT

Server(s) observed running SSH software that support an SSH protocol lower than version 2.

Description
Secure Shell (SSH) is an encrypted network protocol to allow remote login and
other network services to operate securely over an unsecured network by
providing an authenticated and encrypted channel. All modern SSH clients and
servers support the more secure SSH protocol version 2, and any version older
is exploitable and obsolete. Version 1 of the SSH protocol contains
fundamental weaknesses including a design flaw that allows a man-in-the-middle
attack. Findings are removed automatically if they have not been observed for
more than 30 days.

Recommendation
Configure the SSH service to support only SSH protocol version 2 or
higher. Upgrade the SSH service software to the latest version of software.

1 finding

IP ADDRESS	PORT	LAST OBSERVED
2.192.2.157	22	2/8/2022, 3:34:53 PM
Evidence : protocol 1.5		

Telnet Service Observed

-0.3 SCORE IMPACT

We observed Telnet, a remote access service, publicly exposed.

Description
Insecure and/or suspicious Telnet open ports have been detected as being publicly accessible. The availability of these ports allow attackers to engage in authentication bypass attacks (such as brute forcing attempts, remote buffer overflows, blank passwords). An attacker can leverage this access to pivot access into further enterprise resources.

Recommendation
Telnet is an inherently unsafe protocol. Remove the service from the Internet. If a remote access service is necessary, replace Telnet with SSH if possible. If not possible, often the case with older networked hardware, ensure the service is only accessible by VPN.

34 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Cisco telnetd	2.192.6.227	6002	3/8/2022, 11:34:18 PM
Pocket CMD telnetd	2.192.1.63	23	3/8/2022, 10:57:04 PM
BusyBox telnetd	2.192.2.247	23	3/8/2022, 9:50:27 PM
	2.192.0.29	23	3/8/2022, 9:47:15 PM
	2.192.8.131	23	3/8/2022, 9:42:17 PM
	2.192.3.241	23	3/8/2022, 9:30:11 PM
	2.192.1.203	23	3/8/2022, 9:01:41 PM
	2.192.5.160	23	3/8/2022, 8:17:52 PM
	2.192.5.231	23	3/8/2022, 8:15:48 PM
	2.192.2.44	23	3/8/2022, 7:36:28 PM
	2.192.5.8	23	3/8/2022, 7:23:12 PM
BusyBox telnetd	2.192.4.253	23	3/8/2022, 7:22:04 PM
utelnetd	2.192.5.91	23	3/8/2022, 5:34:43 PM
	2.192.4.20	23	3/8/2022, 4:59:31 PM
BusyBox telnetd	2.192.2.247	23	2/24/2022, 3:21:34 PM
BusyBox telnetd	2.192.2.167	8001	2/24/2022, 2:27:49 PM
Linux telnetd	2.192.0.43	8823	2/18/2022, 11:24:25 AM
BusyBox telnetd	2.192.5.182	8001	2/18/2022, 4:23:41 AM
	2.192.11.219	23	2/11/2022, 10:38:50 PM
BusyBox telnetd	2.192.0.21	2332	2/9/2022, 5:08:27 PM
	2.192.9.39	23	2/9/2022, 1:49:39 PM
	2.192.1.54	23	2/8/2022, 11:50:36 PM
BusyBox telnetd	2.192.5.142	23	2/8/2022, 11:36:05 PM
	2.192.0.17	23	2/8/2022, 10:12:36 PM
	2.192.10.24	23	2/8/2022, 10:11:00 PM
BusyBox telnetd	2.192.4.221	23	2/8/2022, 9:32:17 PM
	2.192.11.49	23	2/8/2022, 8:31:41 PM
	2.192.11.219	23	2/8/2022, 7:58:38 PM
	2.192.2.187	23	2/8/2022, 7:46:01 PM
	2.192.7.52	23	2/8/2022, 6:11:52 PM
	2.192.7.32	23	2/8/2022, 6:11:27 PM
	2.192.9.34	23	2/8/2022, 6:06:36 PM
Pocket CMD telnetd	2.192.9.73	23	2/8/2022, 6:05:37 PM
	2.192.3.26	23	2/7/2022, 11:11:00 AM

IP Camera Accessible

-0.2 SCORE IMPACT

We observed an IP Camera, a video or image feed, publicly exposed.

Description
IP cameras allow users to view images and video served through several different protocols, including RTSP, RTP, and HTTP. These cameras use TCP/IP protocol to allow the transmission and viewing of images and video digitally. This

Recommendation
Review the business necessity of exposing a public IP camera feed. Only keep it open when necessary, for example, for a purposely open feed. Even then, you could embed it in a website

enables a number of benefits, including use of local Wi-Fi networks, automated image recognition tied into other systems, use of modern encryption standards, and better image resolution. However, the exposure of such devices to the public internet presents a security and business risk. Place these devices behind firewalls, or otherwise maintain an allow list of IPs that can access them. Only devices with images and video that is truly meant for anyone in the world to view should be publicly accessible. Furthermore, these devices often run on operating systems with unpatched or unknown vulnerabilities, opening up the door for adversaries to compromise the IP camera and pivot throughout an organization's internal network.

without exposing the underlying camera IP. If removal is not possible, consider restricting the service by adding to an allow list the IPs required to access the camera.

8 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Apple AirTunes rtspd	2.192.0.238	554	3/11/2022, 2:38:46 PM
Hikvision IPCam control port	2.192.0.238	8000	3/11/2022, 2:38:46 PM
Hikvision 7513 POE IP camera rtspd	2.192.4.40	554	3/9/2022, 4:23:41 PM
RTSP Service	2.192.0.234	5555	3/5/2022, 9:48:50 PM
D-Link DCS-2130 or Pelco IDE10DN webcam rtspd	2.192.8.33	554	2/24/2022, 4:57:36 PM
Apple AirTunes rtspd	2.192.4.234	1025	2/21/2022, 3:34:17 AM
Mobotix Camera http config	2.192.7.42	8080	2/13/2022, 2:17:41 AM
Hikvision 7513 POE IP camera rtspd	2.192.7.250	554	2/7/2022, 5:01:21 AM

SSH Supports Weak Cipher

-0.3 SCORE IMPACT

A weak cipher has been detected.

Description
The SSH server is configured to support either Arcfour or Cipher Block Chaining (CBC) mode cipher algorithms. SSH can be configured to use Counter (CTR) mode encryption instead of CBC. The use of Arcfour algorithms should be disabled.

Recommendation
Configure the SSH server to disable Arcfour and CBC ciphers.

1 finding

IP ADDRESS	PORT	LAST OBSERVED
2.192.7.28	22	2/24/2022, 2:51:28 PM
Evidence : aes128-cbc		

F 57 PATCHING CADENCE

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the rate at which it takes a company to remediate and apply patches compared to peers.

HIGH SEVERITY		MEDIUM SEVERITY		LOW SEVERITY		POSITIVE
High-Severity Vulnerability in Last Observation	143	Medium Severity CVEs Patching Cadence	1,124	Low Severity CVEs Patching Cadence	64	There are no Positive Signals for Patching Cadence
High Severity CVEs Patching Cadence	319	Medium-Severity Vulnerability in Last Observation	500	Low-Severity Vulnerability in Last Observation	51	

INFORMATIONAL

Low-severity CVE patching analyzed	1
Medium-severity CVE patching analyzed	1
High-severity CVE patching analyzed	1

Low-severity CVE patching analyzed

This analysis reflects the number of low-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.

Description
We analyze patching coverage for low-severity Common Vulnerabilities and Exposures (CVEs). We base this analysis on the number and percentage of low-severity vulnerabilities that were resolved on the network since their detection, and the average resolution time over a 180-day period. You can view these metrics in the table below. Low-severity CVEs have a Common Vulnerability Scoring System (CVSS v2) base score of lower than 4.0. While medium and high-severity vulnerabilities may warrant more urgent attention, maintaining a regular patching cadence for all vulnerabilities is an important security best practice.

Recommendation
Monitor CVE lists and vulnerability repositories for exploit code that may affect the network infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.

1 finding

ALL ACTIVE IN PAST 180 DAYS	RESOLVED ISSUES	RESOLVED %	AVERAGE DAYS TO RESOLVE	RESOLVED: 60 DAYS OR LESS	RESOLVED: 60-120 DAYS	RESOLVED: 121-180 DAYS	RESOLVED: OVER 180 DAYS	LAST UPDATE
147	96	65	46	91	5			3/13/2022, 12:00:00 AM

Medium Severity CVEs Patching Cadence

Medium severity vulnerability seen on network more than 90 days after CVE was published.

-0.6 SCORE IMPACT

Description
Based on scan data, the company had medium severity CVE vulnerability that was open longer than 90 days after the CVE was published. Medium severity CVEs are those with a documented CVSS severity between 4.0 and 6.9. It is best

Recommendation
Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a

practice to mitigate or patch medium severity vulnerabilities within 90 days. Details on each vulnerability are listed in the table below.

regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

500 findings

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2019-20372	2.192.1.62	80	3/12/2022, 3:21:49 AM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2019-20372	2.192.7.64	80	3/11/2022, 11:06:58 PM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2019-6109	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2019-6111	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2017-15906	2.192.2.247	22	3/8/2022, 11:42:35 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-10708	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/21/2018, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2019-6110	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15473	2.192.2.247	22	3/8/2022, 11:42:35 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2020-14145	2.192.2.247	22	3/8/2022, 11:42:35 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-10010	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2018-15919	2.192.2.247	22	3/8/2022, 11:42:35 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2017-15906	2.192.2.167	22	3/8/2022, 11:42:27 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.2.167	22	3/8/2022, 11:42:27 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15919	2.192.2.167	22	3/8/2022, 11:42:27 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2016-10708	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/21/2018, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2019-6111	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6110	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2016-10010	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/4/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2018-15473	2.192.2.167	22	3/8/2022, 11:42:27 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2016-0778	2.192.8.188	22	3/8/2022, 11:26:06 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2017-15906	2.192.8.188	22	3/8/2022, 11:26:06 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-0777	2.192.8.188	22	3/8/2022, 11:26:06 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2020-14145	2.192.8.188	22	3/8/2022, 11:26:06 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15919	2.192.8.188	22	3/8/2022, 11:26:06 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2010-5107	2.192.8.188	22	3/8/2022, 11:26:06 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0777	2.192.2.9	22	3/8/2022, 9:42:01 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2010-5107	2.192.2.9	22	3/8/2022, 9:42:01 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2020-14145	2.192.2.9	22	3/8/2022, 9:42:01 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-0778	2.192.2.9	22	3/8/2022, 9:42:01 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2017-15906	2.192.2.9	22	3/8/2022, 9:42:01 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.2.9	22	3/8/2022, 9:42:01 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.8.91	22	3/8/2022, 9:28:05 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15473	2.192.8.91	22	3/8/2022, 9:28:05 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6111	2.192.8.91	22	3/8/2022, 9:28:05 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6110	2.192.8.91	22	3/8/2022, 9:28:05 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15919	2.192.8.91	22	3/8/2022, 9:28:05 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2017-15906	2.192.8.91	22	3/8/2022, 9:28:05 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6109	2.192.8.91	22	3/8/2022, 9:28:05 AM	1/31/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15919	2.192.10.198	22	3/8/2022, 8:36:38 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.10.198	22	3/8/2022, 8:36:38 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.10.198	22	3/8/2022, 8:36:38 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6110	2.192.10.198	22	3/8/2022, 8:36:38 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2020-14145	2.192.10.198	22	3/8/2022, 8:36:38 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6111	2.192.10.198	22	3/8/2022, 8:36:38 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2020-15778	2.192.6.186	22	3/8/2022, 7:50:00 AM	7/24/2020, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."				
CVE-2020-14145	2.192.6.186	22	3/8/2022, 7:50:00 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2020-12062	2.192.6.186	22	3/8/2022, 7:50:00 AM	6/1/2020, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances."				
CVE-2019-6111	2.192.5.233	22	3/8/2022, 7:43:57 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6110	2.192.5.233	22	3/8/2022, 7:43:57 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15473	2.192.5.233	22	3/8/2022, 7:43:57 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2018-15919	2.192.5.233	22	3/8/2022, 7:43:57 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.5.233	22	3/8/2022, 7:43:57 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2020-14145	2.192.5.233	22	3/8/2022, 7:43:57 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2020-14145	2.192.2.120	22	3/8/2022, 6:04:00 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15919	2.192.2.120	22	3/8/2022, 6:04:00 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2017-15906	2.192.2.120	22	3/8/2022, 6:04:00 AM	10/26/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2014-2653	2.192.2.120	22	3/8/2022, 6:04:00 AM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2015-6564	2.192.2.120	22	3/8/2022, 6:04:00 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2015-5352	2.192.2.120	22	3/8/2022, 6:04:00 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2532	2.192.2.120	22	3/8/2022, 6:04:00 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2016-0778	2.192.2.120	22	3/8/2022, 6:04:00 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2016-0777	2.192.2.120	22	3/8/2022, 6:04:00 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2010-5107	2.192.2.120	22	3/8/2022, 6:04:00 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2015-6564	2.192.2.119	22	3/8/2022, 6:02:46 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2020-14145	2.192.2.119	22	3/8/2022, 6:02:46 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2014-2532	2.192.2.119	22	3/8/2022, 6:02:46 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2010-5107	2.192.2.119	22	3/8/2022, 6:02:46 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0778	2.192.2.119	22	3/8/2022, 6:02:46 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2016-0777	2.192.2.119	22	3/8/2022, 6:02:46 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2014-2653	2.192.2.119	22	3/8/2022, 6:02:46 AM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2015-5352	2.192.2.119	22	3/8/2022, 6:02:46 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2017-15906	2.192.2.119	22	3/8/2022, 6:02:46 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.2.119	22	3/8/2022, 6:02:46 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6110	2.192.4.204	22	3/8/2022, 5:34:05 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15919	2.192.4.204	22	3/8/2022, 5:34:05 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2018-15473	2.192.4.204	22	3/8/2022, 5:34:05 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2020-14145	2.192.4.204	22	3/8/2022, 5:34:05 AM	6/29/2020, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6109	2.192.4.204	22	3/8/2022, 5:34:05 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2019-6111	2.192.4.204	22	3/8/2022, 5:34:05 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2015-5352	2.192.4.31	22	3/8/2022, 5:28:55 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2653	2.192.4.31	22	3/8/2022, 5:28:55 AM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2016-0777	2.192.4.31	22	3/8/2022, 5:28:55 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2015-6564	2.192.4.31	22	3/8/2022, 5:28:55 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2010-5107	2.192.4.31	22	3/8/2022, 5:28:55 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2018-15919	2.192.4.31	22	3/8/2022, 5:28:55 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.4.31	22	3/8/2022, 5:28:55 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2014-2532	2.192.4.31	22	3/8/2022, 5:28:55 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2016-0778	2.192.4.31	22	3/8/2022, 5:28:55 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2017-15906	2.192.4.31	22	3/8/2022, 5:28:55 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.5.95	22	3/8/2022, 12:55:13 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2015-5352	2.192.5.95	22	3/8/2022, 12:55:13 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2653	2.192.5.95	22	3/8/2022, 12:55:13 AM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2015-6564	2.192.5.95	22	3/8/2022, 12:55:13 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2016-0778	2.192.5.95	22	3/8/2022, 12:55:13 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2020-14145	2.192.5.95	22	3/8/2022, 12:55:13 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2017-15906	2.192.5.95	22	3/8/2022, 12:55:13 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-0777	2.192.5.95	22	3/8/2022, 12:55:13 AM	4/1/2016, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2010-5107	2.192.5.95	22	3/8/2022, 12:55:13 AM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2014-2532	2.192.5.95	22	3/8/2022, 12:55:13 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2018-15919	2.192.4.164	22	3/7/2022, 11:25:39 PM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.4.164	22	3/7/2022, 11:25:39 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2017-15906	2.192.4.164	22	3/7/2022, 11:25:39 PM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.4.164	22	3/7/2022, 11:25:39 PM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6110	2.192.4.164	22	3/7/2022, 11:25:39 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2019-6111	2.192.4.164	22	3/7/2022, 11:25:39 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2018-15473	2.192.4.164	22	3/7/2022, 11:25:39 PM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2016-0778	2.192.9.114	22	3/7/2022, 11:12:49 PM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2015-6564	2.192.9.114	22	3/7/2022, 11:12:49 PM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2014-2532	2.192.9.114	22	3/7/2022, 11:12:49 PM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2018-15919	2.192.9.114	22	3/7/2022, 11:12:49 PM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2010-5107	2.192.9.114	22	3/7/2022, 11:12:49 PM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2015-5352	2.192.9.114	22	3/7/2022, 11:12:49 PM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2653	2.192.9.114	22	3/7/2022, 11:12:49 PM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2016-0777	2.192.9.114	22	3/7/2022, 11:12:49 PM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2020-14145	2.192.9.114	22	3/7/2022, 11:12:49 PM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2017-15906	2.192.9.114	22	3/7/2022, 11:12:49 PM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2009-5016	2.192.0.124	8080	2/27/2022, 8:38:21 PM	11/12/2010, 12:00:00 AM
Vulnerability Description : Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.				
CVE-2011-1464	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.				
CVE-2007-1717	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/28/2007, 12:00:00 AM
Vulnerability Description : The mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 truncates e-mail messages at the first ASCIIZ ('\0') byte, which might allow context-dependent attackers to prevent intended information from being delivered in e-mail messages. NOTE: this issue might be security-relevant in cases when the trailing contents of e-mail messages are important, such as logging information or if the message is expected to be well-formed.				
CVE-2007-0988	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/20/2007, 12:00:00 AM
Vulnerability Description : The zend_hash_init function in PHP 5 before 5.2.1 and PHP 4 before 4.4.5, when running on a 64-bit platform, allows context-dependent attackers to cause a denial of service (infinite loop) by unserializing certain integer expressions, which only cause 32-bit arguments to be used after the check for a negative value, as demonstrated by an "a:2147483649:{" argument.				
CVE-2007-1701	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/27/2007, 12:00:00 AM
Vulnerability Description : PHP 4 before 4.4.5, and PHP 5 before 5.2.1, when register_globals is enabled, allows context-dependent attackers to execute arbitrary code via deserialization of session data, which overwrites arbitrary global variables, as demonstrated by calling session_decode on a string beginning with "_SESSIONIs:39:".				
CVE-2011-1470	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.				
CVE-2007-1396	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : The import_request_variables function in PHP 4.0.7 through 4.4.6, and 5.x before 5.2.2, when called without a prefix, does not prevent the (1) GET, (2) POST, (3) COOKIE, (4) FILES, (5) SERVER, (6) SESSION, and other superglobals from being overwritten, which allows remote attackers to spoof source IP address and Referer data, and have other unspecified impact. NOTE: it could be argued that this is a design limitation of PHP and that only the misuse of this feature, i.e. implementation bugs in applications, should be included in CVE. However, it has been fixed by the vendor.				
CVE-2007-1001	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Multiple integer overflows in the (1) createwbmp and (2) readwbmp functions in wbmp.c in the GD library (libgd) in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allow context-dependent attackers to execute arbitrary code via Wireless Bitmap (WBMP) images with large width or height values.				
CVE-2007-0907	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : Buffer underflow in PHP before 5.2.1 allows attackers to cause a denial of service via unspecified vectors involving the sapi_header_op function.				
CVE-2008-3659	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.				
CVE-2007-1884	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Multiple integer signedness errors in the printf function family in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 on 64 bit machines allow context-dependent attackers to execute arbitrary code via (1) certain negative argument numbers that arise in the php_formatted_print function because of 64 to 32 bit truncation, and bypass a check for the maximum allowable value; and (2) a width and precision of -1, which make it possible for the php_sprintf_appendstring function to place an internal buffer at an arbitrary memory location.				
CVE-2007-2510	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/9/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the make_http_soap_request function in PHP before 5.2.2 has unknown impact and remote attack vectors, possibly related to "/" (slash) characters.				
CVE-2011-0421	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.				
CVE-2007-1583	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/21/2007, 12:00:00 AM
Vulnerability Description : The mb_parse_str function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 sets the internal register_globals flag and does not disable it in certain cases when a script terminates, which allows remote attackers to invoke available PHP scripts with register_globals functionality that is not detectable by these scripts, as demonstrated by forcing a memory_limit violation.				
CVE-2012-2143	2.192.0.124	8080	2/27/2022, 8:38:21 PM	7/5/2012, 12:00:00 AM
Vulnerability Description : The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.				
CVE-2008-3660	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.				
CVE-2011-3267	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.				
CVE-2007-1460	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/14/2007, 12:00:00 AM
Vulnerability Description : The zip:// URL wrapper provided by the PECL zip extension in PHP before 4.4.7, and 5.2.0 and 5.2.1, does not implement safemode or open_basedir checks, which allows remote attackers to read ZIP archives located outside of the intended directories.				
CVE-2007-1287	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/6/2007, 12:00:00 AM
Vulnerability Description : A regression error in the phpinfo function in PHP 4.4.3 to 4.4.6, and PHP 6.0 in CVS, allows remote attackers to conduct cross-site scripting (XSS) attacks via GET, POST, or COOKIE array values, which are not escaped in the phpinfo output, as originally fixed for CVE-2005-3388.				
CVE-2011-1467	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.				
CVE-2007-1484	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/16/2007, 12:00:00 AM
Vulnerability Description : The array_user_key_compare function in PHP 4.4.6 and earlier, and 5.x up to 5.2.1, makes erroneous calls to zval_dtor, which triggers memory corruption and allows local users to bypass safe_mode and execute arbitrary code via a certain unset operation after array_user_key_compare has been called.				
CVE-2006-5178	2.192.0.124	8080	2/27/2022, 8:38:21 PM	10/10/2006, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Race condition in the symlink function in PHP 5.1.6 and earlier allows local users to bypass the open_basedir restriction by using a combination of symlink, mkdir, and unlink functions to change the file path after the open_basedir check and before the file is opened by the underlying system, as demonstrated by symlinking a symlink into a subdirectory, to point to a parent directory via .. (dot dot) sequences, and then unlinking the resulting symlink.				
CVE-2007-3304	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/20/2007, 12:00:00 AM
Vulnerability Description : Apache httpd 1.3.37, 2.0.59, and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, aka "SIGUSR1 killer."				
CVE-2007-1475	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/16/2007, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the (1) ibase_connect and (2) ibase_pconnect functions in the interbase extension in PHP 4.4.6 and earlier allow context-dependent attackers to execute arbitrary code via a long argument.				
CVE-2012-3365	2.192.0.124	8080	2/27/2022, 8:38:21 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.				
CVE-2011-1471	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.				
CVE-2012-2336	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2007-1378	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : The ovrimos_longreadlen function in the Ovrimos extension for PHP before 4.4.5 allows context-dependent attackers to write to arbitrary memory locations via the result_id and length arguments.				
CVE-2011-1466	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.				
CVE-2013-1643	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.				
CVE-2007-1379	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : The ovrimos_close function in the Ovrimos extension for PHP before 4.4.5 can trigger efree of an arbitrary address, which might allow context-dependent attackers to execute arbitrary code.				
CVE-2010-4697	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/18/2011, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.				
CVE-2012-0831	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/10/2012, 12:00:00 AM
Vulnerability Description : PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.				
CVE-2007-3799	2.192.0.124	8080	2/27/2022, 8:38:21 PM	7/16/2007, 12:00:00 AM
Vulnerability Description : The session_start function in ext/session in PHP 4.x up to 4.4.7 and 5.x up to 5.2.3 allows remote attackers to insert arbitrary attributes into the session cookie via special characters in a cookie that is obtained from (1) PATH_INFO, (2) the session_id function, and (3) the session_start function, which are not encoded or filtered when the new session cookie is generated, a related issue to CVE-2006-0207.				
CVE-2011-0752	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/2/2011, 12:00:00 AM
Vulnerability Description : The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.				
CVE-2007-6388	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/8/2008, 12:00:00 AM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.				
CVE-2007-3378	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/29/2007, 12:00:00 AM
Vulnerability Description : The (1) session_save_path, (2) ini_set, and (3) error_log functions in PHP 4.4.7 and earlier, and PHP 5 5.2.3 and earlier, when invoked from a .htaccess file, allow remote attackers to bypass safe_mode and open_basedir restrictions and possibly execute arbitrary commands, as demonstrated using (a) php_value, (b) php_flag, and (c) directives in .htaccess.				
CVE-2010-4699	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/18/2011, 12:00:00 AM
Vulnerability Description : The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.				
CVE-2011-3182	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.				
CVE-2009-2626	2.192.0.124	8080	2/27/2022, 8:38:21 PM	12/1/2009, 12:00:00 AM
Vulnerability Description : The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.				
CVE-2008-7068	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/25/2009, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The dba_replace function in PHP 5.2.6 and 4.x allows context-dependent attackers to cause a denial of service (file truncation) via a key with the NULL byte. NOTE: this might only be a vulnerability in limited circumstances in which the attacker can modify or add database entries but does not have permissions to truncate the file.				
CVE-2013-4635	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/21/2013, 12:00:00 AM
Vulnerability Description : Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.				
CVE-2007-1286	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/6/2007, 12:00:00 AM
Vulnerability Description : Integer overflow in PHP 4.4.4 and earlier allows remote context-dependent attackers to execute arbitrary code via a long string to the unserialize function, which triggers the overflow in the ZVAL reference counter.				
CVE-2006-7243	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/18/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.				
CVE-2008-2829	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/23/2008, 12:00:00 AM
Vulnerability Description : php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.				
CVE-2011-1469	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.				
CVE-2012-0883	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/18/2012, 12:00:00 AM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2011-0708	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.				
CVE-2007-2872	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/4/2007, 12:00:00 AM
Vulnerability Description : Multiple integer overflows in the chunk_split function in PHP 5 before 5.2.3 and PHP 4 before 4.4.8 allow remote attackers to cause a denial of service (crash) or execute arbitrary code via the (1) chunks, (2) srclen, and (3) chunklen arguments.				
CVE-2010-3870	2.192.0.124	8080	2/27/2022, 8:38:21 PM	11/12/2010, 12:00:00 AM
Vulnerability Description : The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.				
CVE-2008-0455	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/25/2008, 12:00:00 AM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.				
CVE-2007-1411	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in PHP 4.4.6 and earlier, and unspecified PHP 5 versions, allows local and possibly remote attackers to execute arbitrary code via long server name arguments to the (1) mssql_connect and (2) mssql_pconnect functions.				
CVE-2007-1285	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/6/2007, 12:00:00 AM
Vulnerability Description : The Zend Engine in PHP 4.x before 4.4.7, and 5.x before 5.2.2, allows remote attackers to cause a denial of service (stack exhaustion and PHP crash) via deeply nested arrays, which trigger deep recursion in the variable destruction routines.				
CVE-2011-2202	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/16/2011, 12:00:00 AM
Vulnerability Description : The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."				
CVE-2012-0031	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/18/2012, 12:00:00 AM
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2007-1835	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/3/2007, 12:00:00 AM
Vulnerability Description : PHP 4 before 4.4.5 and PHP 5 before 5.2.1, when using an empty session save path (session.save_path), uses the TMPDIR default after checking the restrictions, which allows local users to bypass open_basedir restrictions.				
CVE-2009-4142	2.192.0.124	8080	2/27/2022, 8:38:21 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.				
CVE-2007-0908	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : The WDDX deserializer in the wddx extension in PHP 5 before 5.2.1 and PHP 4 before 4.4.5 does not properly initialize the key_length variable for a numerical key, which allows context-dependent attackers to read stack memory via a wddxPacket element that contains a variable with a string name before a numerical variable.				
CVE-2008-4107	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/18/2008, 12:00:00 AM
Vulnerability Description : The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.				
CVE-2013-2110	2.192.0.124	8080	2/27/2022, 8:38:21 PM	6/21/2013, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.				
CVE-2007-4652	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/4/2007, 12:00:00 AM
Vulnerability Description : The session extension in PHP before 5.2.4 might allow local users to bypass open_basedir restrictions via a session file that is a symlink.				
CVE-2011-0755	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/2/2011, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.				
CVE-2011-0419	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/16/2011, 12:00:00 AM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2011-0753	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/2/2011, 12:00:00 AM
Vulnerability Description : Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.				
CVE-2007-3998	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/4/2007, 12:00:00 AM
Vulnerability Description : The wordwrap function in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, does not properly use the breakcharlen variable, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash, or infinite loop) via certain arguments, as demonstrated by a 'chr(0), 0, ""' argument set.				
CVE-2007-1582	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/21/2007, 12:00:00 AM
Vulnerability Description : The resource system in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting certain functions in the GD (ext/gd) extension and unspecified other extensions via a userspace error handler, which can be used to destroy and modify internal resources.				
CVE-2007-1710	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/27/2007, 12:00:00 AM
Vulnerability Description : The readfile function in PHP 4.4.4, 5.1.6, and 5.2.1 allows context-dependent attackers to bypass safe_mode restrictions and read arbitrary files by referring to local files with a certain URL syntax instead of a pathname syntax, as demonstrated by a filename preceded a "php://../../" sequence.				
CVE-2007-1380	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : The php_binary serialization handler in the session extension in PHP before 4.4.5, and 5.x before 5.2.1, allows context-dependent attackers to obtain sensitive information (memory contents) via a serialized variable entry with a large length value, which triggers a buffer over-read.				
CVE-2010-4409	2.192.0.124	8080	2/27/2022, 8:38:21 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.				
CVE-2011-1468	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.				
CVE-2011-2483	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.				
CVE-2014-0098	2.192.5.76	80	2/12/2022, 4:34:44 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2018-1312	2.192.5.76	80	2/12/2022, 4:34:44 AM	3/26/2018, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2014-0231	2.192.5.76	80	2/12/2022, 4:34:44 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2016-5387	2.192.5.76	80	2/12/2022, 4:34:44 AM	7/19/2016, 12:00:00 AM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2016-8743	2.192.5.76	80	2/12/2022, 4:34:44 AM	7/27/2017, 12:00:00 AM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2016-4975	2.192.5.76	80	2/12/2022, 4:34:44 AM	8/14/2018, 12:00:00 AM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2017-7529	2.192.3.32	80	2/11/2022, 8:53:59 PM	7/13/2017, 12:00:00 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2019-20372	2.192.3.32	80	2/11/2022, 8:53:59 PM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2018-16845	2.192.3.32	80	2/11/2022, 8:53:59 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2014-3572	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/9/2015, 12:00:00 AM
Vulnerability Description : The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.				
CVE-2008-0891	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/29/2008, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a malformed Client Hello packet. NOTE: some of these details are obtained from third party information.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2018-1312	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/26/2018, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2010-0434	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/5/2010, 12:00:00 AM
Vulnerability Description : The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.				
CVE-2011-1470	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.				
CVE-2015-1788	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.				
CVE-2011-1464	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.				
CVE-2015-0293	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.				
CVE-2010-2100	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/27/2010, 12:00:00 AM
Vulnerability Description : The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strtr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2006-7243	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/18/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.				
CVE-2015-1791	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.				
CVE-2011-3607	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/8/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.				
CVE-2008-7270	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.				
CVE-2016-5387	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/19/2016, 12:00:00 AM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2015-0288	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.				
CVE-2009-1272	2.192.3.142	80	2/11/2022, 8:52:12 PM	4/8/2009, 12:00:00 AM
Vulnerability Description : The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.				
CVE-2014-0224	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/5/2014, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.				
CVE-2008-4107	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/18/2008, 12:00:00 AM
Vulnerability Description : The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.				
CVE-2010-1861	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The sysvshm extension for PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to write to arbitrary memory addresses by using an object's __sleep function to interrupt an internal call to the shm_put_var function, which triggers access of a freed resource.				
CVE-2014-3506	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2014, 12:00:00 AM
Vulnerability Description : d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.				
CVE-2010-2101	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/27/2010, 12:00:00 AM
Vulnerability Description : The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2008-5498	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/26/2008, 12:00:00 AM
Vulnerability Description : Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2009-5016	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/12/2010, 12:00:00 AM
Vulnerability Description : Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.				
CVE-2011-0421	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.				
CVE-2011-0755	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/2/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.				
CVE-2011-4577	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.				
CVE-2012-1171	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/15/2014, 12:00:00 AM
Vulnerability Description : The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.				
CVE-2011-1469	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.				
CVE-2018-19935	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/7/2018, 12:00:00 AM
Vulnerability Description : ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.				
CVE-2015-0287	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.				
CVE-2014-0238	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/1/2014, 12:00:00 AM
Vulnerability Description : The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.				
CVE-2011-4885	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/30/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.				
CVE-2012-3365	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.				
CVE-2011-2483	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.				
CVE-2010-5298	2.192.3.142	80	2/11/2022, 8:52:12 PM	4/14/2014, 12:00:00 AM
Vulnerability Description : Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.				
CVE-2009-1195	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/28/2009, 12:00:00 AM
Vulnerability Description : The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.				
CVE-2014-0195	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/5/2014, 12:00:00 AM
Vulnerability Description : The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.				
CVE-2010-4657	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/13/2019, 12:00:00 AM
Vulnerability Description : PHP5 before 5.4.4 allows passing invalid utf-8 strings via the xmlTextWriterWriteAttribute, which are then misparsed by libxml2. This results in memory leak into the resulting output.				
CVE-2015-1790	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.				
CVE-2011-4718	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2013, 12:00:00 AM
Vulnerability Description : Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.				
CVE-2009-3557	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/23/2009, 12:00:00 AM
Vulnerability Description : The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.				
CVE-2014-3570	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/9/2015, 12:00:00 AM
Vulnerability Description : The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.				
CVE-2009-4418	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/24/2009, 12:00:00 AM
Vulnerability Description : The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.				
CVE-2011-1467	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.				
CVE-2010-2190	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/8/2010, 12:00:00 AM
Vulnerability Description : The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2008-1678	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/10/2008, 12:00:00 AM
Vulnerability Description : Memory leak in the zlib_stateful_init function in crypto/comp/c_zlib.c in libssl in OpenSSL 0.9.8f through 0.9.8h allows remote attackers to cause a denial of service (memory consumption) via multiple calls, as demonstrated by initial SSL client handshakes to the Apache HTTP Server mod_ssl that specify a compression algorithm.				
CVE-2013-2110	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/21/2013, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.				
CVE-2014-0221	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/5/2014, 12:00:00 AM
Vulnerability Description : The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.				
CVE-2010-2191	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/8/2010, 12:00:00 AM
Vulnerability Description : The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.				
CVE-2011-4576	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.				
CVE-2010-3065	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/20/2010, 12:00:00 AM
Vulnerability Description : The default session serializer in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 does not properly handle the PS_UNDEF_MARKER marker, which allows context-dependent attackers to modify arbitrary session variables via a crafted session variable name.				
CVE-2010-1862	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2010-2484	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/20/2010, 12:00:00 AM
Vulnerability Description : The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.				
CVE-2010-1860	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The html_entity_decode function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.				
CVE-2010-1128	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.				
CVE-2009-4355	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/14/2010, 12:00:00 AM
Vulnerability Description : Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.				
CVE-2010-3870	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/12/2010, 12:00:00 AM
Vulnerability Description : The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.				
CVE-2010-2531	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/20/2010, 12:00:00 AM
Vulnerability Description : The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.				
CVE-2011-1468	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.				
CVE-2015-0209	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.				
CVE-2009-3558	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/23/2009, 12:00:00 AM
Vulnerability Description : The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.				
CVE-2012-0831	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/10/2012, 12:00:00 AM
Vulnerability Description : PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.				
CVE-2014-0231	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2013-4635	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/21/2013, 12:00:00 AM
Vulnerability Description : Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.				
CVE-2014-3505	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2014, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.				
CVE-2012-1165	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/15/2012, 12:00:00 AM
Vulnerability Description : The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.				
CVE-2010-1864	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The addcslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2010-3710	2.192.3.142	80	2/11/2022, 8:52:12 PM	10/25/2010, 12:00:00 AM
Vulnerability Description : Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.				
CVE-2009-2626	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/1/2009, 12:00:00 AM
Vulnerability Description : The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.				
CVE-2012-0883	2.192.3.142	80	2/11/2022, 8:52:12 PM	4/18/2012, 12:00:00 AM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2015-8994	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/2/2017, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.				
CVE-2008-3659	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.				
CVE-2011-1466	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.				
CVE-2013-1643	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.				
CVE-2015-1792	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.				
CVE-2010-2093	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/27/2010, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the request shutdown functionality in PHP 5.2 before 5.2.13 and 5.3 before 5.3.2 allows context-dependent attackers to cause a denial of service (crash) via a stream context structure that is freed before destruction occurs.				
CVE-2012-1172	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/24/2012, 12:00:00 AM
Vulnerability Description : The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.				
CVE-2012-0027	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.				
CVE-2014-3568	2.192.3.142	80	2/11/2022, 8:52:12 PM	10/19/2014, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.				
CVE-2009-1378	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/19/2009, 12:00:00 AM
Vulnerability Description : Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."				
CVE-2011-4108	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.				
CVE-2011-0752	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/2/2011, 12:00:00 AM
Vulnerability Description : The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.				
CVE-2009-4142	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.				
CVE-2006-7250	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/29/2012, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.				
CVE-2011-3267	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.				
CVE-2014-3510	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2014, 12:00:00 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.				
CVE-2016-0703	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/2/2016, 12:00:00 AM
Vulnerability Description : The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2010-0740	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.				
CVE-2012-0031	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/18/2012, 12:00:00 AM
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2012-0789	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/14/2012, 12:00:00 AM
Vulnerability Description : Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.				
CVE-2012-2333	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/14/2012, 12:00:00 AM
Vulnerability Description : Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.				
CVE-2014-3508	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2014, 12:00:00 AM
Vulnerability Description : The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.				
CVE-2011-4619	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.				
CVE-2010-4697	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/18/2011, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.				
CVE-2014-3470	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/5/2014, 12:00:00 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.				
CVE-2011-3210	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/22/2011, 12:00:00 AM
Vulnerability Description : The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.				
CVE-2011-1473	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/16/2012, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.				
CVE-2011-0708	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/20/2011, 12:00:00 AM
Vulnerability Description : exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.				
CVE-2008-1384	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/27/2008, 12:00:00 AM
Vulnerability Description : Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a printf format parameter with a large width specifier, related to the php_sprintf_appendstring function in formatted_print.c and probably other functions for formatted strings (aka *printf functions).				
CVE-2010-4645	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/11/2011, 12:00:00 AM
Vulnerability Description : strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.				
CVE-2010-1915	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/12/2010, 12:00:00 AM
Vulnerability Description : The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.				
CVE-2012-0053	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/28/2012, 12:00:00 AM
Vulnerability Description : protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.				
CVE-2014-0237	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/1/2014, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.				
CVE-2014-3571	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/9/2015, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.				
CVE-2011-0419	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/16/2011, 12:00:00 AM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2016-8743	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/27/2017, 12:00:00 AM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2010-1917	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/12/2010, 12:00:00 AM
Vulnerability Description : Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.				
CVE-2009-3555	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/9/2009, 12:00:00 AM
Vulnerability Description : The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.				
CVE-2009-0789	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/27/2009, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.				
CVE-2010-3709	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/9/2010, 12:00:00 AM
Vulnerability Description : The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.				
CVE-2016-4975	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/14/2018, 12:00:00 AM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2010-1914	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/12/2010, 12:00:00 AM
Vulnerability Description : The Zend Engine in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information by interrupting the handler for the (1) ZEND_BW_XOR opcode (shift_left_function), (2) ZEND_SL opcode (bitwise_xor_function), or (3) ZEND_SR opcode (shift_right_function), related to the convert_to_long_base function.				
CVE-2008-2666	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/20/2008, 12:00:00 AM
Vulnerability Description : Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.				
CVE-2014-0098	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/18/2014, 12:00:00 AM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2016-0704	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/2/2016, 12:00:00 AM
Vulnerability Description : An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2011-3182	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.				
CVE-2009-1271	2.192.3.142	80	2/11/2022, 8:52:12 PM	4/8/2009, 12:00:00 AM
Vulnerability Description : The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.				
CVE-2009-1386	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/4/2009, 12:00:00 AM
Vulnerability Description : ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.				
CVE-2015-0289	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.				
CVE-2018-19520	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/25/2018, 12:00:00 AM
Vulnerability Description : An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.				
CVE-2009-1377	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/19/2009, 12:00:00 AM
Vulnerability Description : The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2009-1387	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/4/2009, 12:00:00 AM
Vulnerability Description : The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."				
CVE-2012-0057	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/2/2012, 12:00:00 AM
Vulnerability Description : PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.				
CVE-2014-2497	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/21/2014, 12:00:00 AM
Vulnerability Description : The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.				
CVE-2013-4248	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/18/2013, 12:00:00 AM
Vulnerability Description : The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2012-0788	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/14/2012, 12:00:00 AM
Vulnerability Description : The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.				
CVE-2010-2097	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/27/2010, 12:00:00 AM
Vulnerability Description : The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2017-3735	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/28/2017, 12:00:00 AM
Vulnerability Description : While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.				
CVE-2010-1130	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).				
CVE-2008-2829	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/23/2008, 12:00:00 AM
Vulnerability Description : php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.				
CVE-2015-1789	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.				
CVE-2012-0884	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/13/2012, 12:00:00 AM
Vulnerability Description : The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.				
CVE-2008-5077	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/7/2009, 12:00:00 AM
Vulnerability Description : OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.				
CVE-2009-0590	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/27/2009, 12:00:00 AM
Vulnerability Description : The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.				
CVE-2007-4850	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/25/2008, 12:00:00 AM
Vulnerability Description : curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence, a different vulnerability than CVE-2006-2563.				
CVE-2011-4354	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/27/2012, 12:00:00 AM
Vulnerability Description : crypto/bn/bn_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.				
CVE-2016-7478	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/11/2017, 12:00:00 AM
Vulnerability Description : Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.				
CVE-2012-2336	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2014-8275	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/9/2015, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.				
CVE-2018-19396	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/20/2018, 12:00:00 AM
Vulnerability Description : ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.				
CVE-2013-0166	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/8/2013, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.				
CVE-2010-4699	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/18/2011, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.				
CVE-2010-0433	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/5/2010, 12:00:00 AM
Vulnerability Description : The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.				
CVE-2014-3507	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/13/2014, 12:00:00 AM
Vulnerability Description : Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.				
CVE-2012-2143	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/5/2012, 12:00:00 AM
Vulnerability Description : The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.				
CVE-2010-4180	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.				
CVE-2008-3660	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.				
CVE-2017-7529	2.192.3.235	80	2/11/2022, 8:49:40 PM	7/13/2017, 12:00:00 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2019-20372	2.192.3.235	80	2/11/2022, 8:49:40 PM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2018-16845	2.192.3.235	80	2/11/2022, 8:49:40 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2018-16845	2.192.4.54	80	2/11/2022, 1:43:31 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2017-7529	2.192.4.54	80	2/11/2022, 1:43:31 PM	7/13/2017, 12:00:00 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2019-20372	2.192.4.54	80	2/11/2022, 1:43:31 PM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2019-11038	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/19/2019, 12:00:00 AM
Vulnerability Description : When using the gdImageCreateFromXbm() function in the GD Graphics Library (aka LibGD) 2.2.5, as used in the PHP GD extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.				
CVE-2019-11045	2.192.3.2	80	2/11/2022, 2:44:31 AM	12/23/2019, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP DirectoryIterator class accepts filenames with embedded \0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.				
CVE-2018-0735	2.192.3.2	80	2/11/2022, 2:44:31 AM	10/29/2018, 12:00:00 AM
Vulnerability Description : The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).				
CVE-2018-19935	2.192.3.2	80	2/11/2022, 2:44:31 AM	12/7/2018, 12:00:00 AM
Vulnerability Description : ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.				
CVE-2018-0732	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/12/2018, 12:00:00 AM
Vulnerability Description : During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).				
CVE-2020-7060	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/10/2020, 12:00:00 AM
Vulnerability Description : When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2020-7064	2.192.3.2	80	2/11/2022, 2:44:31 AM	4/1/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.				
CVE-2020-7063	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/27/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.				
CVE-2019-11036	2.192.3.2	80	2/11/2022, 2:44:31 AM	5/3/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.				
CVE-2018-20783	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/21/2019, 12:00:00 AM
Vulnerability Description : In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.				
CVE-2019-11047	2.192.3.2	80	2/11/2022, 2:44:31 AM	12/23/2019, 12:00:00 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-14883	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/3/2018, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.				
CVE-2019-10081	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/15/2019, 12:00:00 AM
Vulnerability Description : HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.				
CVE-2020-9490	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/7/2020, 12:00:00 AM
Vulnerability Description : Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.				
CVE-2019-11050	2.192.3.2	80	2/11/2022, 2:44:31 AM	12/23/2019, 12:00:00 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-1333	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/18/2018, 12:00:00 AM
Vulnerability Description : By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).				
CVE-2019-10082	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/26/2019, 12:00:00 AM
Vulnerability Description : In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.				
CVE-2020-7066	2.192.3.2	80	2/11/2022, 2:44:31 AM	4/1/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.29, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.				
CVE-2020-7069	2.192.3.2	80	2/11/2022, 2:44:31 AM	10/2/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.				
CVE-2020-7070	2.192.3.2	80	2/11/2022, 2:44:31 AM	10/2/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.				
CVE-2015-9253	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/19/2018, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.				
CVE-2019-9639	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/9/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.				
CVE-2019-9022	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries.				
CVE-2019-0220	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/11/2019, 12:00:00 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2019-11041	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/9/2019, 12:00:00 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-14851	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/2/2018, 12:00:00 AM
Vulnerability Description : exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.				
CVE-2019-11042	2.192.3.2	80	2/11/2022, 2:44:31 AM	8/9/2019, 12:00:00 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-17082	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/16/2018, 12:00:00 AM
Vulnerability Description : The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.				
CVE-2019-0197	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/11/2019, 12:00:00 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.				
CVE-2019-9637	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/9/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.				
CVE-2018-11763	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/25/2018, 12:00:00 AM
Vulnerability Description : In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.				
CVE-2019-9638	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/9/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.				
CVE-2019-0196	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/11/2019, 12:00:00 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.				
CVE-2019-1543	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/6/2019, 12:00:00 AM
Vulnerability Description : ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k (Affected 1.1.0-1.1.0j).				
CVE-2019-6977	2.192.3.2	80	2/11/2022, 2:44:31 AM	1/27/2019, 12:00:00 AM
Vulnerability Description : gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.				
CVE-2019-9024	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.				
CVE-2018-0737	2.192.3.2	80	2/11/2022, 2:44:31 AM	4/16/2018, 12:00:00 AM
Vulnerability Description : The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).				
CVE-2018-0734	2.192.3.2	80	2/11/2022, 2:44:31 AM	10/30/2018, 12:00:00 AM
Vulnerability Description : The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).				
CVE-2019-9640	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/9/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.				
CVE-2019-11040	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/19/2019, 12:00:00 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2020-7062	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/27/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.				
CVE-2020-7059	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/10/2020, 12:00:00 AM
Vulnerability Description : When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2019-11039	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/19/2019, 12:00:00 AM
Vulnerability Description : Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.				
CVE-2019-1563	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/10/2019, 12:00:00 AM
Vulnerability Description : In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2019-20372	2.192.2.24	80	2/11/2022, 2:25:44 AM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2017-7529	2.192.2.24	80	2/11/2022, 2:25:44 AM	7/13/2017, 12:00:00 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-16845	2.192.2.24	80	2/11/2022, 2:25:44 AM	11/7/2018, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2015-0293	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.				
CVE-2011-4619	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.				
CVE-2011-3607	2.192.9.190	80	2/10/2022, 11:59:49 AM	11/8/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.				
CVE-2015-1792	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.				
CVE-2015-0209	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.				
CVE-2010-4180	2.192.9.190	80	2/10/2022, 11:59:49 AM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.				
CVE-2012-0883	2.192.9.190	80	2/10/2022, 11:59:49 AM	4/18/2012, 12:00:00 AM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2016-0703	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/2/2016, 12:00:00 AM
Vulnerability Description : The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2012-1165	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/15/2012, 12:00:00 AM
Vulnerability Description : The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.				
CVE-2015-1788	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.				
CVE-2010-5298	2.192.9.190	80	2/10/2022, 11:59:49 AM	4/14/2014, 12:00:00 AM
Vulnerability Description : Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.				
CVE-2014-3507	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/13/2014, 12:00:00 AM
Vulnerability Description : Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.				
CVE-2016-5387	2.192.9.190	80	2/10/2022, 11:59:49 AM	7/19/2016, 12:00:00 AM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2014-8275	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/9/2015, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.				
CVE-2014-0224	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/5/2014, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.				
CVE-2015-0288	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.				
CVE-2014-3470	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/5/2014, 12:00:00 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.				
CVE-2012-2333	2.192.9.190	80	2/10/2022, 11:59:49 AM	5/14/2012, 12:00:00 AM
Vulnerability Description : Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2011-1473	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/16/2012, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.				
CVE-2011-0419	2.192.9.190	80	2/10/2022, 11:59:49 AM	5/16/2011, 12:00:00 AM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2014-0231	2.192.9.190	80	2/10/2022, 11:59:49 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2015-0287	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.				
CVE-2016-4975	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/14/2018, 12:00:00 AM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2011-4576	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.				
CVE-2012-0053	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/28/2012, 12:00:00 AM
Vulnerability Description : protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.				
CVE-2011-4577	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.				
CVE-2012-0884	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/13/2012, 12:00:00 AM
Vulnerability Description : The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.				
CVE-2014-3570	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/9/2015, 12:00:00 AM
Vulnerability Description : The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.				
CVE-2015-1790	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.				
CVE-2011-0014	2.192.9.190	80	2/10/2022, 11:59:49 AM	2/19/2011, 12:00:00 AM
Vulnerability Description : ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka "OCSP stapling vulnerability."				
CVE-2014-3568	2.192.9.190	80	2/10/2022, 11:59:49 AM	10/19/2014, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.				
CVE-2014-0195	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/5/2014, 12:00:00 AM
Vulnerability Description : The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.				
CVE-2015-1791	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.				
CVE-2014-3508	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/13/2014, 12:00:00 AM
Vulnerability Description : The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.				
CVE-2010-0740	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/26/2010, 12:00:00 AM
Vulnerability Description : The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.				
CVE-2006-7250	2.192.9.190	80	2/10/2022, 11:59:49 AM	2/29/2012, 12:00:00 AM
Vulnerability Description : The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.				
CVE-2016-0704	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/2/2016, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2014-3571	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/9/2015, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.				
CVE-2010-0434	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/5/2010, 12:00:00 AM
Vulnerability Description : The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.				
CVE-2011-4108	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.				
CVE-2015-0289	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.				
CVE-2014-0098	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2014-3506	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/13/2014, 12:00:00 AM
Vulnerability Description : d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.				
CVE-2010-0433	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/5/2010, 12:00:00 AM
Vulnerability Description : The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.				
CVE-2012-0027	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.				
CVE-2014-3505	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/13/2014, 12:00:00 AM
Vulnerability Description : Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.				
CVE-2014-3572	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/9/2015, 12:00:00 AM
Vulnerability Description : The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.				
CVE-2017-3735	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/28/2017, 12:00:00 AM
Vulnerability Description : While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.				
CVE-2018-1312	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/26/2018, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2012-0031	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/18/2012, 12:00:00 AM
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2015-1789	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.				
CVE-2011-3210	2.192.9.190	80	2/10/2022, 11:59:49 AM	9/22/2011, 12:00:00 AM
Vulnerability Description : The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.				
CVE-2014-3510	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/13/2014, 12:00:00 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.				
CVE-2013-0166	2.192.9.190	80	2/10/2022, 11:59:49 AM	2/8/2013, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.				
CVE-2014-0221	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/5/2014, 12:00:00 AM
Vulnerability Description : The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.				
CVE-2016-8743	2.192.9.190	80	2/10/2022, 11:59:49 AM	7/27/2017, 12:00:00 AM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2017-7529	2.192.4.71	80	2/10/2022, 9:57:17 AM	7/13/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-16845	2.192.4.71	80	2/10/2022, 9:57:17 AM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2019-20372	2.192.4.71	80	2/10/2022, 9:57:17 AM	1/9/2020, 12:00:00 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2018-15919	2.192.4.184	22	2/8/2022, 3:36:45 PM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2017-15906	2.192.4.184	22	2/8/2022, 3:36:45 PM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6111	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6109	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2016-10010	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2016-10708	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/21/2018, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2018-15473	2.192.4.184	22	2/8/2022, 3:36:45 PM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2020-14145	2.192.4.184	22	2/8/2022, 3:36:45 PM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6110	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15919	2.192.4.252	22	2/8/2022, 3:35:18 PM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2017-15906	2.192.4.252	22	2/8/2022, 3:35:18 PM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2010-5107	2.192.4.252	22	2/8/2022, 3:35:18 PM	3/7/2013, 12:00:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0777	2.192.4.252	22	2/8/2022, 3:35:18 PM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2016-0778	2.192.4.252	22	2/8/2022, 3:35:18 PM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2020-14145	2.192.4.252	22	2/8/2022, 3:35:18 PM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15473	2.192.4.221	22	2/8/2022, 10:15:59 AM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2016-10708	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/21/2018, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2019-6109	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/31/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2019-6111	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2017-15906	2.192.4.221	22	2/8/2022, 10:15:59 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-10010	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2018-15919	2.192.4.221	22	2/8/2022, 10:15:59 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.4.221	22	2/8/2022, 10:15:59 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6110	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2020-15778	2.192.6.117	22	2/8/2022, 8:04:21 AM	7/24/2020, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."				
CVE-2020-14145	2.192.6.117	22	2/8/2022, 8:04:21 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2020-12062	2.192.6.117	22	2/8/2022, 8:04:21 AM	6/1/2020, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances."				
CVE-2014-2532	2.192.11.227	22	2/8/2022, 7:40:14 AM	3/18/2014, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2016-0777	2.192.11.227	22	2/8/2022, 7:40:14 AM	4/1/2016, 12:00:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2015-6564	2.192.11.227	22	2/8/2022, 7:40:14 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2014-2653	2.192.11.227	22	2/8/2022, 7:40:14 AM	3/27/2014, 12:00:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2018-15919	2.192.11.227	22	2/8/2022, 7:40:14 AM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2015-5352	2.192.11.227	22	2/8/2022, 7:40:14 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2017-15906	2.192.11.227	22	2/8/2022, 7:40:14 AM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-0778	2.192.11.227	22	2/8/2022, 7:40:14 AM	1/14/2016, 12:00:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2020-14145	2.192.11.227	22	2/8/2022, 7:40:14 AM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2010-5107	2.192.11.227	22	2/8/2022, 7:40:14 AM	3/7/2013, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2019-6111	2.192.8.230	22	2/7/2022, 11:56:47 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2018-15473	2.192.8.230	22	2/7/2022, 11:56:47 PM	8/17/2018, 12:00:00 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6110	2.192.8.230	22	2/7/2022, 11:56:47 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2017-15906	2.192.8.230	22	2/7/2022, 11:56:47 PM	10/26/2017, 12:00:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.8.230	22	2/7/2022, 11:56:47 PM	6/29/2020, 12:00:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15919	2.192.8.230	22	2/7/2022, 11:56:47 PM	8/28/2018, 12:00:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.8.230	22	2/7/2022, 11:56:47 PM	1/31/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				

Low Severity CVEs Patching Cadence

-0.2 SCORE IMPACT

Low severity vulnerability seen network more than 120 days after CVE was published.

Description

Based on scan data, the company had low severity CVE vulnerability that was open longer than 120 days after the CVE was published. Low severity CVEs are those with a documented CVSS severity under 4.0. It is best practice to mitigate or patch high severity vulnerabilities within 120 days. Details on each vulnerability are listed in the table below.

Recommendation

Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

64 findings

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-10011	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2018-20685	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2018-20685	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2011-5000	2.192.8.188	22	3/8/2022, 11:26:06 AM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.8.188	22	3/8/2022, 11:26:06 AM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-4327	2.192.2.9	22	3/8/2022, 9:42:01 AM	2/3/2014, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-5000	2.192.2.9	22	3/8/2022, 9:42:01 AM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2018-20685	2.192.8.91	22	3/8/2022, 9:28:05 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2018-20685	2.192.10.198	22	3/8/2022, 8:36:38 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2018-20685	2.192.5.233	22	3/8/2022, 7:43:57 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.2.120	22	3/8/2022, 6:04:00 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2015-6563	2.192.2.119	22	3/8/2022, 6:02:46 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.4.204	22	3/8/2022, 5:34:05 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.4.31	22	3/8/2022, 5:28:55 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2015-6563	2.192.5.95	22	3/8/2022, 12:55:13 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.4.164	22	3/7/2022, 11:25:39 PM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.9.114	22	3/7/2022, 11:12:49 PM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2007-2509	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/9/2007, 12:00:00 AM
Vulnerability Description : CRLF injection vulnerability in the ftp_putcmd function in PHP before 4.4.7, and 5.x before 5.2.2 allows remote attackers to inject arbitrary FTP commands via CRLF sequences in the parameters to earlier FTP commands.				
CVE-2008-5814	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/2/2009, 12:00:00 AM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.				
CVE-2006-4625	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/12/2006, 12:00:00 AM
Vulnerability Description : PHP 4.x up to 4.4.4 and PHP 5 up to 5.1.6 allows local users to bypass certain Apache HTTP Server httpd.conf options, such as safe_mode and open_basedir, via the ini_restore function, which resets the values to their php.ini (Master Value) defaults.				
CVE-2007-2727	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/16/2007, 12:00:00 AM
Vulnerability Description : The mcrypt_create_iv function in ext/mcrypt/mcrypt.c in PHP before 4.4.7, 5.2.1, and possibly 5.0.x and other PHP 5 versions, calls php_rand_r with an uninitialized seed variable and therefore always generates the same initialization vector (IV), which might allow context-dependent attackers to decrypt certain data more easily because of the guessable encryption keys.				
CVE-2008-0456	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/25/2008, 12:00:00 AM
Vulnerability Description : CRLF injection vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.				
CVE-2014-5459	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/27/2014, 12:00:00 AM
Vulnerability Description : The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.				
CVE-2012-2687	2.192.5.76	80	2/12/2022, 4:34:44 AM	8/22/2012, 12:00:00 AM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2016-7056	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/10/2018, 12:00:00 AM
Vulnerability Description : A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.				
CVE-2014-5459	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/27/2014, 12:00:00 AM
Vulnerability Description : The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2011-1945	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/31/2011, 12:00:00 AM
Vulnerability Description : The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.				
CVE-2012-2687	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/22/2012, 12:00:00 AM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2014-0076	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/25/2014, 12:00:00 AM
Vulnerability Description : The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.				
CVE-2013-0169	2.192.3.142	80	2/11/2022, 8:52:12 PM	2/8/2013, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.				
CVE-2011-4415	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/8/2011, 12:00:00 AM
Vulnerability Description : The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.				
CVE-2008-5814	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/2/2009, 12:00:00 AM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.				
CVE-2019-1552	2.192.3.2	80	2/11/2022, 2:44:31 AM	7/30/2019, 12:00:00 AM
Vulnerability Description : OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2018-5407	2.192.3.2	80	2/11/2022, 2:44:31 AM	11/15/2018, 12:00:00 AM
Vulnerability Description : Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.				
CVE-2020-7068	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/9/2020, 12:00:00 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.				
CVE-2019-1547	2.192.3.2	80	2/11/2022, 2:44:31 AM	9/10/2019, 12:00:00 AM
Vulnerability Description : Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2011-1945	2.192.9.190	80	2/10/2022, 11:59:49 AM	5/31/2011, 12:00:00 AM
Vulnerability Description : The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.				
CVE-2014-0076	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/25/2014, 12:00:00 AM
Vulnerability Description : The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.				
CVE-2011-4415	2.192.9.190	80	2/10/2022, 11:59:49 AM	11/8/2011, 12:00:00 AM
Vulnerability Description : The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.				
CVE-2013-0169	2.192.9.190	80	2/10/2022, 11:59:49 AM	2/8/2013, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.				
CVE-2012-2687	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/22/2012, 12:00:00 AM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2016-7056	2.192.9.190	80	2/10/2022, 11:59:49 AM	9/10/2018, 12:00:00 AM
Vulnerability Description : A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.				
CVE-2018-20685	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/10/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2011-5000	2.192.4.252	22	2/8/2022, 3:35:18 PM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.4.252	22	2/8/2022, 3:35:18 PM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2018-20685	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2015-6563	2.192.11.227	22	2/8/2022, 7:40:14 AM	8/24/2015, 12:00:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.8.230	22	2/7/2022, 11:56:47 PM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2011-5000	2.192.9.81	2222	1/15/2022, 11:15:32 PM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.9.81	2222	1/15/2022, 11:15:32 PM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2012-0814	2.192.9.81	2222	1/15/2022, 11:15:32 PM	1/27/2012, 12:00:00 AM
Vulnerability Description : The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.				
CVE-2018-20685	2.192.5.195	22	1/15/2022, 1:33:16 PM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.5.195	22	1/15/2022, 1:33:16 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2011-4327	2.192.6.49	22	1/15/2022, 1:28:00 AM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-5000	2.192.6.49	22	1/15/2022, 1:28:00 AM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2012-0814	2.192.8.82	2222	1/14/2022, 9:29:32 PM	1/27/2012, 12:00:00 AM
Vulnerability Description : The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.				
CVE-2011-4327	2.192.8.82	2222	1/14/2022, 9:29:32 PM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-5000	2.192.8.82	2222	1/14/2022, 9:29:32 PM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2018-20685	2.192.0.241	22	1/14/2022, 11:57:36 AM	1/10/2019, 12:00:00 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2011-4327	2.192.1.217	22	1/14/2022, 8:03:53 AM	2/3/2014, 12:00:00 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-5000	2.192.1.217	22	1/14/2022, 8:03:53 AM	4/5/2012, 12:00:00 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				

Medium-Severity Vulnerability in Last Observation

-0.5 SCORE IMPACT

We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

Description

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability.
Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

Recommendation

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

500 findings

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2019-20372	2.192.1.62	80	1/9/2020, 12:00:00 AM	3/12/2022, 3:21:49 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2019-20372	2.192.7.64	80	1/9/2020, 12:00:00 AM	3/11/2022, 11:06:58 PM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2020-14145	2.192.2.247	22	6/29/2020, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15919	2.192.2.247	22	8/28/2018, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6110	2.192.2.247	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2016-10010	2.192.2.247	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2017-15906	2.192.2.247	22	10/26/2017, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6111	2.192.2.247	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2016-10708	2.192.2.247	22	1/21/2018, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2019-6109	2.192.2.247	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.2.247	22	8/17/2018, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6109	2.192.2.167	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15919	2.192.2.167	22	8/28/2018, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.2.167	22	6/29/2020, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2018-15473	2.192.2.167	22	8/17/2018, 12:00:00 AM	3/8/2022, 11:42:27 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6111	2.192.2.167	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6110	2.192.2.167	22	1/31/2019, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2016-10010	2.192.2.167	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2016-10708	2.192.2.167	22	1/21/2018, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2017-15906	2.192.2.167	22	10/26/2017, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2017-15906	2.192.8.188	22	10/26/2017, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.8.188	22	6/29/2020, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-0777	2.192.8.188	22	4/1/2016, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2016-0778	2.192.8.188	22	1/14/2016, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2010-5107	2.192.8.188	22	3/7/2013, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2018-15919	2.192.8.188	22	8/28/2018, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2016-0778	2.192.2.9	22	1/14/2016, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2016-0777	2.192.2.9	22	4/1/2016, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2017-15906	2.192.2.9	22	10/26/2017, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.2.9	22	6/29/2020, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2010-5107	2.192.2.9	22	3/7/2013, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2018-15919	2.192.2.9	22	8/28/2018, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2018-15919	2.192.8.91	22	8/28/2018, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.8.91	22	6/29/2020, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6110	2.192.8.91	22	1/31/2019, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2017-15906	2.192.8.91	22	10/26/2017, 12:00:00 AM	3/8/2022, 9:28:05 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6111	2.192.8.91	22	1/31/2019, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6109	2.192.8.91	22	1/31/2019, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.8.91	22	8/17/2018, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2018-15919	2.192.10.198	22	8/28/2018, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2020-14145	2.192.10.198	22	6/29/2020, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6111	2.192.10.198	22	1/31/2019, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2019-6109	2.192.10.198	22	1/31/2019, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2019-6110	2.192.10.198	22	1/31/2019, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15473	2.192.10.198	22	8/17/2018, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2020-12062	2.192.6.186	22	6/1/2020, 12:00:00 AM	3/8/2022, 7:50:00 AM
Vulnerability Description : ** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances."				
CVE-2020-15778	2.192.6.186	22	7/24/2020, 12:00:00 AM	3/8/2022, 7:50:00 AM
Vulnerability Description : ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."				
CVE-2020-14145	2.192.6.186	22	6/29/2020, 12:00:00 AM	3/8/2022, 7:50:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6109	2.192.5.233	22	1/31/2019, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.5.233	22	8/17/2018, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6111	2.192.5.233	22	1/31/2019, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2018-15919	2.192.5.233	22	8/28/2018, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6110	2.192.5.233	22	1/31/2019, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2020-14145	2.192.5.233	22	6/29/2020, 12:00:00 AM	3/8/2022, 7:43:57 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2010-5107	2.192.2.120	22	3/7/2013, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2014-2653	2.192.2.120	22	3/27/2014, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2016-0777	2.192.2.120	22	4/1/2016, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2015-5352	2.192.2.120	22	8/3/2015, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2015-6564	2.192.2.120	22	8/24/2015, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2020-14145	2.192.2.120	22	6/29/2020, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2017-15906	2.192.2.120	22	10/26/2017, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-0778	2.192.2.120	22	1/14/2016, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2018-15919	2.192.2.120	22	8/28/2018, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2014-2532	2.192.2.120	22	3/18/2014, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2016-0778	2.192.2.119	22	1/14/2016, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2020-14145	2.192.2.119	22	6/29/2020, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2014-2532	2.192.2.119	22	3/18/2014, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2017-15906	2.192.2.119	22	10/26/2017, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.2.119	22	8/28/2018, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2015-6564	2.192.2.119	22	8/24/2015, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2015-5352	2.192.2.119	22	8/3/2015, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2653	2.192.2.119	22	3/27/2014, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2016-0777	2.192.2.119	22	4/1/2016, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2010-5107	2.192.2.119	22	3/7/2013, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2019-6110	2.192.4.204	22	1/31/2019, 12:00:00 AM	3/8/2022, 5:34:05 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2020-14145	2.192.4.204	22	6/29/2020, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6111	2.192.4.204	22	1/31/2019, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2018-15919	2.192.4.204	22	8/28/2018, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6109	2.192.4.204	22	1/31/2019, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.4.204	22	8/17/2018, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2015-6564	2.192.4.31	22	8/24/2015, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2016-0777	2.192.4.31	22	4/1/2016, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2014-2532	2.192.4.31	22	3/18/2014, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2020-14145	2.192.4.31	22	6/29/2020, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2010-5107	2.192.4.31	22	3/7/2013, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0778	2.192.4.31	22	1/14/2016, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2018-15919	2.192.4.31	22	8/28/2018, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2015-5352	2.192.4.31	22	8/3/2015, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2014-2653	2.192.4.31	22	3/27/2014, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2017-15906	2.192.4.31	22	10/26/2017, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2020-14145	2.192.5.95	22	6/29/2020, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2010-5107	2.192.5.95	22	3/7/2013, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0778	2.192.5.95	22	1/14/2016, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2014-2653	2.192.5.95	22	3/27/2014, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2016-0777	2.192.5.95	22	4/1/2016, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-2532	2.192.5.95	22	3/18/2014, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2015-5352	2.192.5.95	22	8/3/2015, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2018-15919	2.192.5.95	22	8/28/2018, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2015-6564	2.192.5.95	22	8/24/2015, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2017-15906	2.192.5.95	22	10/26/2017, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.4.164	22	8/28/2018, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2017-15906	2.192.4.164	22	10/26/2017, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6111	2.192.4.164	22	1/31/2019, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2020-14145	2.192.4.164	22	6/29/2020, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6109	2.192.4.164	22	1/31/2019, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2018-15473	2.192.4.164	22	8/17/2018, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6110	2.192.4.164	22	1/31/2019, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2015-6564	2.192.9.114	22	8/24/2015, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2020-14145	2.192.9.114	22	6/29/2020, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-0777	2.192.9.114	22	4/1/2016, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2018-15919	2.192.9.114	22	8/28/2018, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2014-2532	2.192.9.114	22	3/18/2014, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2010-5107	2.192.9.114	22	3/7/2013, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2014-2653	2.192.9.114	22	3/27/2014, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2015-5352	2.192.9.114	22	8/3/2015, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2016-0778	2.192.9.114	22	1/14/2016, 12:00:00 AM	3/7/2022, 11:12:49 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2017-15906	2.192.9.114	22	10/26/2017, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2010-4697	2.192.0.124	8080	1/18/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.				
CVE-2012-3365	2.192.0.124	8080	7/20/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.				
CVE-2011-1467	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.				
CVE-2007-0908	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The WDDX deserializer in the wddx extension in PHP 5 before 5.2.1 and PHP 4 before 4.4.5 does not properly initialize the key_length variable for a numerical key, which allows context-dependent attackers to read stack memory via a wddxPacket element that contains a variable with a string name before a numerical variable.				
CVE-2007-3378	2.192.0.124	8080	6/29/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The (1) session_save_path, (2) ini_set, and (3) error_log functions in PHP 4.4.7 and earlier, and PHP 5 5.2.3 and earlier, when invoked from a .htaccess file, allow remote attackers to bypass safe_mode and open_basedir restrictions and possibly execute arbitrary commands, as demonstrated using (a) php_value, (b) php_flag, and (c) directives in .htaccess.				
CVE-2007-1460	2.192.0.124	8080	3/14/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The zip:// URL wrapper provided by the PECL zip extension in PHP before 4.4.7, and 5.2.0 and 5.2.1, does not implement safemode or open_basedir checks, which allows remote attackers to read ZIP archives located outside of the intended directories.				
CVE-2010-4409	2.192.0.124	8080	12/6/2010, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.				
CVE-2012-0831	2.192.0.124	8080	2/10/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.				
CVE-2007-0907	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer underflow in PHP before 5.2.1 allows attackers to cause a denial of service via unspecified vectors involving the sapi_header_op function.				
CVE-2011-1466	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.				
CVE-2007-3799	2.192.0.124	8080	7/16/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The session_start function in ext/session in PHP 4.x up to 4.4.7 and 5.x up to 5.2.3 allows remote attackers to insert arbitrary attributes into the session cookie via special characters in a cookie that is obtained from (1) PATH_INFO, (2) the session_id function, and (3) the session_start function, which are not encoded or filtered when the new session cookie is generated, a related issue to CVE-2006-0207.				
CVE-2011-0708	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.				
CVE-2013-4635	2.192.0.124	8080	6/21/2013, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.				
CVE-2011-0419	2.192.0.124	8080	5/16/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2011-1469	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.				
CVE-2007-3998	2.192.0.124	8080	9/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The wordwrap function in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, does not properly use the breakcharlen variable, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash, or infinite loop) via certain arguments, as demonstrated by a 'chr(0), 0, ""' argument set.				
CVE-2007-1717	2.192.0.124	8080	3/28/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 truncates e-mail messages at the first ASCIIZ ('\0') byte, which might allow context-dependent attackers to prevent intended information from being delivered in e-mail messages. NOTE: this issue might be security-relevant in cases when the trailing contents of e-mail messages are important, such as logging information or if the message is expected to be well-formed.				
CVE-2007-1379	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The ovrimos_close function in the Ovrimos extension for PHP before 4.4.5 can trigger efree of an arbitrary address, which might allow context-dependent attackers to execute arbitrary code.				
CVE-2011-2483	2.192.0.124	8080	8/25/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.				
CVE-2008-0455	2.192.0.124	8080	1/25/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.				
CVE-2008-3660	2.192.0.124	8080	8/15/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.				
CVE-2007-1835	2.192.0.124	8080	4/3/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4 before 4.4.5 and PHP 5 before 5.2.1, when using an empty session save path (session.save_path), uses the TMPDIR default after checking the restrictions, which allows local users to bypass open_basedir restrictions.				
CVE-2011-3182	2.192.0.124	8080	8/25/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.				
CVE-2008-4107	2.192.0.124	8080	9/18/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.				
CVE-2012-2143	2.192.0.124	8080	7/5/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.				
CVE-2011-1471	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.				
CVE-2007-1380	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The php_binary serialization handler in the session extension in PHP before 4.4.5, and 5.x before 5.2.1, allows context-dependent attackers to obtain sensitive information (memory contents) via a serialized variable entry with a large length value, which triggers a buffer over-read.				
CVE-2010-3870	2.192.0.124	8080	11/12/2010, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.				
CVE-2011-3267	2.192.0.124	8080	8/25/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.				
CVE-2011-0753	2.192.0.124	8080	2/2/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.				
CVE-2007-3304	2.192.0.124	8080	6/20/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Apache httpd 1.3.37, 2.0.59, and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, aka "SIGUSR1 killer."				
CVE-2013-1643	2.192.0.124	8080	3/6/2013, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.				
CVE-2007-1710	2.192.0.124	8080	3/27/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The readfile function in PHP 4.4.4, 5.1.6, and 5.2.1 allows context-dependent attackers to bypass safe_mode restrictions and read arbitrary files by referring to local files with a certain URL syntax instead of a pathname syntax, as demonstrated by a filename preceded a "php://../../" sequence.				
CVE-2011-0752	2.192.0.124	8080	2/2/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.				
CVE-2007-6388	2.192.0.124	8080	1/8/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.				
CVE-2007-1583	2.192.0.124	8080	3/21/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The mb_parse_str function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 sets the internal register_globals flag and does not disable it in certain cases when a script terminates, which allows remote attackers to invoke available PHP scripts with register_globals functionality that is not detectable by these scripts, as demonstrated by forcing a memory_limit violation.				
CVE-2006-5178	2.192.0.124	8080	10/10/2006, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Race condition in the symlink function in PHP 5.1.6 and earlier allows local users to bypass the open_basedir restriction by using a combination of symlink, mkdir, and unlink functions to change the file path after the open_basedir check and before the file is opened by the underlying system, as demonstrated by symlinking a symlink into a subdirectory, to point to a parent directory via .. (dot dot) sequences, and then unlinking the resulting symlink.				
CVE-2007-1286	2.192.0.124	8080	3/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in PHP 4.4.4 and earlier allows remote context-dependent attackers to execute arbitrary code via a long string to the unserialize function, which triggers the overflow in the ZVAL reference counter.				
CVE-2009-5016	2.192.0.124	8080	11/12/2010, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.				
CVE-2012-0031	2.192.0.124	8080	1/18/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2009-4142	2.192.0.124	8080	12/21/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.				
CVE-2007-0988	2.192.0.124	8080	2/20/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The zend_hash_init function in PHP 5 before 5.2.1 and PHP 4 before 4.4.5, when running on a 64-bit platform, allows context-dependent attackers to cause a denial of service (infinite loop) by unserializing certain integer expressions, which only cause 32-bit arguments to be used after the check for a negative value, as demonstrated by an "a:2147483649:{" argument.				
CVE-2008-3659	2.192.0.124	8080	8/15/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.				
CVE-2007-1484	2.192.0.124	8080	3/16/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The array_user_key_compare function in PHP 4.4.6 and earlier, and 5.x up to 5.2.1, makes erroneous calls to zval_dtor, which triggers memory corruption and allows local users to bypass safe_mode and execute arbitrary code via a certain unset operation after array_user_key_compare has been called.				
CVE-2011-1470	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.				
CVE-2008-7068	2.192.0.124	8080	8/25/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The dba_replace function in PHP 5.2.6 and 4.x allows context-dependent attackers to cause a denial of service (file truncation) via a key with the NULL byte. NOTE: this might only be a vulnerability in limited circumstances in which the attacker can modify or add database entries but does not have permissions to truncate the file.				
CVE-2012-0883	2.192.0.124	8080	4/18/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2009-2626	2.192.0.124	8080	12/1/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.				
CVE-2011-1468	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.				
CVE-2007-1701	2.192.0.124	8080	3/27/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4 before 4.4.5, and PHP 5 before 5.2.1, when register_globals is enabled, allows context-dependent attackers to execute arbitrary code via deserialization of session data, which overwrites arbitrary global variables, as demonstrated by calling session_decode on a string beginning with "_SESSION\s:39:".				
CVE-2007-1378	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The ovrimos_longreadlen function in the Ovrimos extension for PHP before 4.4.5 allows context-dependent attackers to write to arbitrary memory locations via the result_id and length arguments.				
CVE-2007-1001	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple integer overflows in the (1) createwbmp and (2) readwbmp functions in wbmp.c in the GD library (libgd) in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allow context-dependent attackers to execute arbitrary code via Wireless Bitmap (WBMP) images with large width or height values.				
CVE-2007-1582	2.192.0.124	8080	3/21/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The resource system in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting certain functions in the GD (ext/gd) extension and unspecified other extensions via a userspace error handler, which can be used to destroy and modify internal resources.				
CVE-2007-2510	2.192.0.124	8080	5/9/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the make_http_soap_request function in PHP before 5.2.2 has unknown impact and remote attack vectors, possibly related to "/" (slash) characters.				
CVE-2011-1464	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.				
CVE-2007-2872	2.192.0.124	8080	6/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple integer overflows in the chunk_split function in PHP 5 before 5.2.3 and PHP 4 before 4.4.8 allow remote attackers to cause a denial of service (crash) or execute arbitrary code via the (1) chunks, (2) srclen, and (3) chunklen arguments.				
CVE-2013-2110	2.192.0.124	8080	6/21/2013, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.				
CVE-2007-1287	2.192.0.124	8080	3/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : A regression error in the phpinfo function in PHP 4.4.3 to 4.4.6, and PHP 6.0 in CVS, allows remote attackers to conduct cross-site scripting (XSS) attacks via GET, POST, or COOKIE array values, which are not escaped in the phpinfo output, as originally fixed for CVE-2005-3388.				
CVE-2011-0421	2.192.0.124	8080	3/20/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.				
CVE-2007-1285	2.192.0.124	8080	3/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The Zend Engine in PHP 4.x before 4.4.7, and 5.x before 5.2.2, allows remote attackers to cause a denial of service (stack exhaustion and PHP crash) via deeply nested arrays, which trigger deep recursion in the variable destruction routines.				
CVE-2008-2829	2.192.0.124	8080	6/23/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.				
CVE-2007-1411	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in PHP 4.4.6 and earlier, and unspecified PHP 5 versions, allows local and possibly remote attackers to execute arbitrary code via long server name arguments to the (1) mssql_connect and (2) mssql_pconnect functions.				
CVE-2006-7243	2.192.0.124	8080	1/18/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.				
CVE-2007-1475	2.192.0.124	8080	3/16/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple buffer overflows in the (1) ibase_connect and (2) ibase_pconnect functions in the interbase extension in PHP 4.4.6 and earlier allow context-dependent attackers to execute arbitrary code via a long argument.				
CVE-2010-4699	2.192.0.124	8080	1/18/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.				
CVE-2007-1884	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple integer signedness errors in the printf function family in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 on 64 bit machines allow context-dependent attackers to execute arbitrary code via (1) certain negative argument numbers that arise in the php_formatted_print function because of 64 to 32 bit truncation, and bypass a check for the maximum allowable value; and (2) a width and precision of -1, which make it possible for the php_sprintf_appendstring function to place an internal buffer at an arbitrary memory location.				
CVE-2007-1396	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The import_request_variables function in PHP 4.0.7 through 4.4.6, and 5.x before 5.2.2, when called without a prefix, does not prevent the (1) GET, (2) POST, (3) COOKIE, (4) FILES, (5) SERVER, (6) SESSION, and other superglobals from being overwritten, which allows remote attackers to spoof source IP address and Referer data, and have other unspecified impact. NOTE: it could be argued that this is a design limitation of PHP and that only the misuse of this feature, i.e. implementation bugs in applications, should be included in CVE. However, it has been fixed by the vendor.				
CVE-2011-2202	2.192.0.124	8080	6/16/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."				
CVE-2007-4652	2.192.0.124	8080	9/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The session extension in PHP before 5.2.4 might allow local users to bypass open_basedir restrictions via a session file that is a symlink.				
CVE-2012-2336	2.192.0.124	8080	5/11/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2011-0755	2.192.0.124	8080	2/2/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.				
CVE-2018-1312	2.192.5.76	80	3/26/2018, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2014-0098	2.192.5.76	80	3/18/2014, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2016-8743	2.192.5.76	80	7/27/2017, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2014-0231	2.192.5.76	80	7/20/2014, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2016-4975	2.192.5.76	80	8/14/2018, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2016-5387	2.192.5.76	80	7/19/2016, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2019-20372	2.192.3.32	80	1/9/2020, 12:00:00 AM	2/11/2022, 8:53:59 PM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2017-7529	2.192.3.32	80	7/13/2017, 12:00:00 AM	2/11/2022, 8:53:59 PM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-16845	2.192.3.32	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:53:59 PM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-0098	2.192.3.142	80	3/18/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2011-1469	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.				
CVE-2008-5498	2.192.3.142	80	12/26/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.				
CVE-2010-1128	2.192.3.142	80	3/26/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.				
CVE-2015-1791	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.				
CVE-2012-0057	2.192.3.142	80	2/2/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.				
CVE-2018-1312	2.192.3.142	80	3/26/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2011-4354	2.192.3.142	80	1/27/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : crypto/bn/bn_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.				
CVE-2014-0221	2.192.3.142	80	6/5/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.				
CVE-2008-3659	2.192.3.142	80	8/15/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.				
CVE-2010-5298	2.192.3.142	80	4/14/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.				
CVE-2012-0788	2.192.3.142	80	2/14/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.				
CVE-2010-1917	2.192.3.142	80	5/12/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.				
CVE-2008-4107	2.192.3.142	80	9/18/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) rand and (2) mt_rand functions in PHP 5.2.6 do not produce cryptographically strong random numbers, which allows attackers to leverage exposures in products that rely on these functions for security-relevant functionality, as demonstrated by the password-reset functionality in Joomla! 1.5.x and WordPress before 2.6.2, a different vulnerability than CVE-2008-2107, CVE-2008-2108, and CVE-2008-4102.				
CVE-2010-4645	2.192.3.142	80	1/11/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.				
CVE-2010-1864	2.192.3.142	80	5/7/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The addcslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2011-4885	2.192.3.142	80	12/30/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.				
CVE-2015-0209	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.				
CVE-2015-1792	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.				
CVE-2012-0883	2.192.3.142	80	4/18/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2007-4850	2.192.3.142	80	1/25/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : curl/interface.c in the cURL library (aka libcurl) in PHP 5.2.4 and 5.2.5 allows context-dependent attackers to bypass safe_mode and open_basedir restrictions and read arbitrary files via a file:// request containing a \x00 sequence, a different vulnerability than CVE-2006-2563.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2009-3557	2.192.3.142	80	11/23/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The tempnam function in ext/standard/file.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass safe_mode restrictions, and create files in group-writable or world-writable directories, via the dir and prefix arguments.				
CVE-2014-0195	2.192.3.142	80	6/5/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.				
CVE-2011-3210	2.192.3.142	80	9/22/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.				
CVE-2009-1272	2.192.3.142	80	4/8/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The php_zip_make_relative_path function in php_zip.c in PHP 5.2.x before 5.2.9 allows context-dependent attackers to cause a denial of service (crash) via a ZIP file that contains filenames with relative paths, which is not properly handled during extraction.				
CVE-2014-3572	2.192.3.142	80	1/9/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.				
CVE-2016-4975	2.192.3.142	80	8/14/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2015-1790	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.				
CVE-2012-2336	2.192.3.142	80	5/11/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2014-3570	2.192.3.142	80	1/9/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.				
CVE-2011-3607	2.192.3.142	80	11/8/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.				
CVE-2006-7250	2.192.3.142	80	2/29/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.				
CVE-2010-4657	2.192.3.142	80	11/13/2019, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP5 before 5.4.4 allows passing invalid utf-8 strings via the xmlTextWriterWriteAttribute, which are then misparsed by libxml2. This results in memory leak into the resulting output.				
CVE-2014-3506	2.192.3.142	80	8/13/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.				
CVE-2010-1130	2.192.3.142	80	3/26/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).				
CVE-2017-3735	2.192.3.142	80	8/28/2017, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.				
CVE-2016-0704	2.192.3.142	80	3/2/2016, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2010-0433	2.192.3.142	80	3/5/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.				
CVE-2016-0703	2.192.3.142	80	3/2/2016, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2010-2484	2.192.3.142	80	8/20/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.				
CVE-2009-3555	2.192.3.142	80	11/9/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.				
CVE-2012-2143	2.192.3.142	80	7/5/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.				
CVE-2015-0287	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.				
CVE-2011-1470	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.				
CVE-2014-0237	2.192.3.142	80	6/1/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.				
CVE-2013-4635	2.192.3.142	80	6/21/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.				
CVE-2014-3510	2.192.3.142	80	8/13/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.				
CVE-2008-1384	2.192.3.142	80	3/27/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a printf format parameter with a large width specifier, related to the php_sprintf_appendstring function in formatted_print.c and probably other functions for formatted strings (aka *printf functions).				
CVE-2012-0789	2.192.3.142	80	2/14/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.				
CVE-2012-0831	2.192.3.142	80	2/10/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.				
CVE-2011-1468	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.				
CVE-2011-4718	2.192.3.142	80	8/13/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.				
CVE-2010-3065	2.192.3.142	80	8/20/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The default session serializer in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 does not properly handle the PS_UNDEF_MARKER marker, which allows context-dependent attackers to modify arbitrary session variables via a crafted session variable name.				
CVE-2010-4697	2.192.3.142	80	1/18/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.				
CVE-2015-1788	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.				
CVE-2010-4180	2.192.3.142	80	12/6/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.				
CVE-2015-8994	2.192.3.142	80	3/2/2017, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.				
CVE-2011-3267	2.192.3.142	80	8/25/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.				
CVE-2014-0238	2.192.3.142	80	6/1/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.				
CVE-2012-1165	2.192.3.142	80	3/15/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.				
CVE-2015-0288	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.				
CVE-2009-0789	2.192.3.142	80	3/27/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.				
CVE-2018-19520	2.192.3.142	80	11/25/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.				
CVE-2014-3507	2.192.3.142	80	8/13/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.				
CVE-2011-4576	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.				
CVE-2014-0231	2.192.3.142	80	7/20/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2018-19396	2.192.3.142	80	11/20/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.				
CVE-2010-1862	2.192.3.142	80	5/7/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2010-1915	2.192.3.142	80	5/12/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.				
CVE-2010-2100	2.192.3.142	80	5/27/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strtr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2016-8743	2.192.3.142	80	7/27/2017, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2011-1467	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.				
CVE-2009-0590	2.192.3.142	80	3/27/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.				
CVE-2010-2097	2.192.3.142	80	5/27/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2010-2093	2.192.3.142	80	5/27/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Use-after-free vulnerability in the request shutdown functionality in PHP 5.2 before 5.2.13 and 5.3 before 5.3.2 allows context-dependent attackers to cause a denial of service (crash) via a stream context structure that is freed before destruction occurs.				
CVE-2010-2101	2.192.3.142	80	5/27/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2016-5387	2.192.3.142	80	7/19/2016, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2009-1378	2.192.3.142	80	5/19/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."				
CVE-2010-0434	2.192.3.142	80	3/5/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.				
CVE-2009-1377	2.192.3.142	80	5/19/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."				
CVE-2014-3505	2.192.3.142	80	8/13/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.				
CVE-2013-1643	2.192.3.142	80	3/6/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The SOAP parser in PHP before 5.3.23 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-1824.				
CVE-2010-0740	2.192.3.142	80	3/26/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.				
CVE-2011-4619	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.				
CVE-2012-2333	2.192.3.142	80	5/14/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.				
CVE-2014-3571	2.192.3.142	80	1/9/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.				
CVE-2013-0166	2.192.3.142	80	2/8/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.				
CVE-2008-5077	2.192.3.142	80	1/7/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.				
CVE-2013-4248	2.192.3.142	80	8/18/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2011-4577	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.				
CVE-2016-7478	2.192.3.142	80	1/11/2017, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.				
CVE-2010-2531	2.192.3.142	80	8/20/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.				
CVE-2011-1473	2.192.3.142	80	6/16/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : ** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.				
CVE-2014-8275	2.192.3.142	80	1/9/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.				
CVE-2011-0708	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.				
CVE-2014-3508	2.192.3.142	80	8/13/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.				
CVE-2009-3558	2.192.3.142	80	11/23/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.				
CVE-2011-0419	2.192.3.142	80	5/16/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2014-0224	2.192.3.142	80	6/5/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.				
CVE-2015-0293	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.				
CVE-2014-3568	2.192.3.142	80	10/19/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.				
CVE-2012-0053	2.192.3.142	80	1/28/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.				
CVE-2011-0421	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.				
CVE-2011-1464	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.				
CVE-2009-1195	2.192.3.142	80	5/28/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.				
CVE-2008-3660	2.192.3.142	80	8/15/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP 4.4.x before 4.4.9, and 5.x through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.				
CVE-2009-1271	2.192.3.142	80	4/8/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The JSON_parser function (ext/json/JSON_parser.c) in PHP 5.2.x before 5.2.9 allows remote attackers to cause a denial of service (segmentation fault) via a malformed string to the json_decode API function.				
CVE-2008-2829	2.192.3.142	80	6/23/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : php_imap.c in PHP 5.2.5, 5.2.6, 4.x, and other versions, uses obsolete API calls that allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long IMAP request, which triggers an "rfc822.c legacy routine buffer overflow" error message, related to the rfc822_write_address function.				
CVE-2008-2666	2.192.3.142	80	6/20/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.				
CVE-2008-1678	2.192.3.142	80	7/10/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Memory leak in the zlib_stateful_init function in crypto/comp/c_zlib.c in libssl in OpenSSL 0.9.8f through 0.9.8h allows remote attackers to cause a denial of service (memory consumption) via multiple calls, as demonstrated by initial SSL client handshakes to the Apache HTTP Server mod_ssl that specify a compression algorithm.				
CVE-2012-0884	2.192.3.142	80	3/13/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.				
CVE-2012-1171	2.192.3.142	80	2/15/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.				
CVE-2009-4142	2.192.3.142	80	12/21/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The htmlspecialchars function in PHP before 5.2.12 does not properly handle (1) overlong UTF-8 sequences, (2) invalid Shift_JIS sequences, and (3) invalid EUC-JP sequences, which allows remote attackers to conduct cross-site scripting (XSS) attacks by placing a crafted byte sequence before a special character.				
CVE-2012-0031	2.192.3.142	80	1/18/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2011-0755	2.192.3.142	80	2/2/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.				
CVE-2009-5016	2.192.3.142	80	11/12/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP before 5.2.11 makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.				
CVE-2010-4699	2.192.3.142	80	1/18/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.				
CVE-2013-2110	2.192.3.142	80	6/21/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.				
CVE-2009-4418	2.192.3.142	80	12/24/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The unserialize function in PHP 5.3.0 and earlier allows context-dependent attackers to cause a denial of service (resource consumption) via a deeply nested serialized variable, as demonstrated by a string beginning with a:1: followed by many {a:1: sequences.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2010-3870	2.192.3.142	80	11/12/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.				
CVE-2010-3710	2.192.3.142	80	10/25/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.				
CVE-2010-1860	2.192.3.142	80	5/7/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The html_entity_decode function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.				
CVE-2012-1172	2.192.3.142	80	5/24/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.				
CVE-2008-7270	2.192.3.142	80	12/6/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.				
CVE-2014-3470	2.192.3.142	80	6/5/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.				
CVE-2011-1466	2.192.3.142	80	3/20/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.				
CVE-2010-1861	2.192.3.142	80	5/7/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The sysvshm extension for PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to write to arbitrary memory addresses by using an object's __sleep function to interrupt an internal call to the shm_put_var function, which triggers access of a freed resource.				
CVE-2010-3709	2.192.3.142	80	11/9/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.				
CVE-2010-2191	2.192.3.142	80	6/8/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.				
CVE-2015-0289	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.				
CVE-2012-0027	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.				
CVE-2009-1387	2.192.3.142	80	6/4/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."				
CVE-2009-1386	2.192.3.142	80	6/4/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.				
CVE-2008-0891	2.192.3.142	80	5/29/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a malformed Client Hello packet. NOTE: some of these details are obtained from third party information.				
CVE-2010-1914	2.192.3.142	80	5/12/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Zend Engine in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information by interrupting the handler for the (1) ZEND_BW_XOR opcode (shift_left_function), (2) ZEND_SL opcode (bitwise_xor_function), or (3) ZEND_SR opcode (shift_right_function), related to the convert_to_long_base function.				
CVE-2010-2190	2.192.3.142	80	6/8/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.				
CVE-2012-3365	2.192.3.142	80	7/20/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.				
CVE-2011-4108	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.				
CVE-2011-3182	2.192.3.142	80	8/25/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.				
CVE-2011-0752	2.192.3.142	80	2/2/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.				
CVE-2006-7243	2.192.3.142	80	1/18/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.				
CVE-2015-1789	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.				
CVE-2011-2483	2.192.3.142	80	8/25/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.				
CVE-2014-2497	2.192.3.142	80	3/21/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.				
CVE-2009-2626	2.192.3.142	80	12/1/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.				
CVE-2009-4355	2.192.3.142	80	1/14/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_cleanup_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.				
CVE-2018-19935	2.192.3.142	80	12/7/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.				
CVE-2017-7529	2.192.3.235	80	7/13/2017, 12:00:00 AM	2/11/2022, 8:49:40 PM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2019-20372	2.192.3.235	80	1/9/2020, 12:00:00 AM	2/11/2022, 8:49:40 PM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2018-16845	2.192.3.235	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:49:40 PM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2019-20372	2.192.4.54	80	1/9/2020, 12:00:00 AM	2/11/2022, 1:43:31 PM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2018-16845	2.192.4.54	80	11/7/2018, 12:00:00 AM	2/11/2022, 1:43:31 PM
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2017-7529	2.192.4.54	80	7/13/2017, 12:00:00 AM	2/11/2022, 1:43:31 PM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-20783	2.192.3.2	80	2/21/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.				
CVE-2019-11038	2.192.3.2	80	6/19/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When using the gdImageCreateFromXbm() function in the GD Graphics Library (aka LibGD) 2.2.5, as used in the PHP GD extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.				
CVE-2019-0220	2.192.3.2	80	6/11/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.				
CVE-2020-7064	2.192.3.2	80	4/1/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.				
CVE-2020-7059	2.192.3.2	80	2/10/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2019-10081	2.192.3.2	80	8/15/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.				
CVE-2018-14851	2.192.3.2	80	8/2/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.				
CVE-2020-7070	2.192.3.2	80	10/2/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.				
CVE-2015-9253	2.192.3.2	80	2/19/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.				
CVE-2020-9490	2.192.3.2	80	8/7/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.				
CVE-2019-0196	2.192.3.2	80	6/11/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.				
CVE-2019-9024	2.192.3.2	80	2/22/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.				
CVE-2019-11036	2.192.3.2	80	5/3/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.				
CVE-2019-0197	2.192.3.2	80	6/11/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.				
CVE-2020-7066	2.192.3.2	80	4/1/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.29, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.				
CVE-2020-7063	2.192.3.2	80	2/27/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.				
CVE-2019-11050	2.192.3.2	80	12/23/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-0732	2.192.3.2	80	6/12/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).				
CVE-2018-19935	2.192.3.2	80	12/7/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.				
CVE-2019-10082	2.192.3.2	80	9/26/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.				
CVE-2019-1543	2.192.3.2	80	3/6/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k (Affected 1.1.0-1.1.0j).				
CVE-2019-9640	2.192.3.2	80	3/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.				
CVE-2020-7062	2.192.3.2	80	2/27/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.				
CVE-2019-9022	2.192.3.2	80	2/22/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries.				
CVE-2018-1333	2.192.3.2	80	6/18/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).				
CVE-2018-17082	2.192.3.2	80	9/16/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.				
CVE-2019-11042	2.192.3.2	80	8/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2019-9638	2.192.3.2	80	3/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.				
CVE-2018-11763	2.192.3.2	80	9/25/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.				
CVE-2019-11041	2.192.3.2	80	8/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2020-7069	2.192.3.2	80	10/2/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.				
CVE-2018-0735	2.192.3.2	80	10/29/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).				
CVE-2018-14883	2.192.3.2	80	8/3/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.				
CVE-2019-6977	2.192.3.2	80	1/27/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.				
CVE-2019-11039	2.192.3.2	80	6/19/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.				
CVE-2019-11040	2.192.3.2	80	6/19/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2019-1563	2.192.3.2	80	9/10/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2019-11045	2.192.3.2	80	12/23/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP DirectoryIterator class accepts filenames with embedded \0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.				
CVE-2020-7060	2.192.3.2	80	2/10/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2019-9639	2.192.3.2	80	3/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.				
CVE-2018-0737	2.192.3.2	80	4/16/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).				
CVE-2019-9637	2.192.3.2	80	3/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.				
CVE-2019-11047	2.192.3.2	80	12/23/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.				
CVE-2018-0734	2.192.3.2	80	10/30/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).				
CVE-2019-20372	2.192.2.24	80	1/9/2020, 12:00:00 AM	2/11/2022, 2:25:44 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2017-7529	2.192.2.24	80	7/13/2017, 12:00:00 AM	2/11/2022, 2:25:44 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-16845	2.192.2.24	80	11/7/2018, 12:00:00 AM	2/11/2022, 2:25:44 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2014-3470	2.192.9.190	80	6/5/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.				
CVE-2011-3210	2.192.9.190	80	9/22/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) via out-of-order messages that violate the TLS protocol.				
CVE-2010-0434	2.192.9.190	80	3/5/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.				
CVE-2014-8275	2.192.9.190	80	1/9/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.				
CVE-2013-0166	2.192.9.190	80	2/8/2013, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.				
CVE-2011-4619	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.				
CVE-2011-1473	2.192.9.190	80	6/16/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : ** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.				
CVE-2014-0098	2.192.9.190	80	3/18/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.				
CVE-2011-4108	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.				
CVE-2015-0287	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.				
CVE-2012-1165	2.192.9.190	80	3/15/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.				
CVE-2015-1788	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.				
CVE-2014-3571	2.192.9.190	80	1/9/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.				
CVE-2011-3607	2.192.9.190	80	11/8/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.				
CVE-2014-0231	2.192.9.190	80	7/20/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.				
CVE-2011-0419	2.192.9.190	80	5/16/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.				
CVE-2014-0224	2.192.9.190	80	6/5/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.				
CVE-2010-4180	2.192.9.190	80	12/6/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.				
CVE-2017-3735	2.192.9.190	80	8/28/2017, 12:00:00 AM	2/10/2022, 11:59:49 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.				
CVE-2015-0293	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.				
CVE-2006-7250	2.192.9.190	80	2/29/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.				
CVE-2015-0209	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.				
CVE-2010-5298	2.192.9.190	80	4/14/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.				
CVE-2014-3568	2.192.9.190	80	10/19/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.				
CVE-2012-0883	2.192.9.190	80	4/18/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.				
CVE-2012-0053	2.192.9.190	80	1/28/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.				
CVE-2011-4577	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.				
CVE-2014-3510	2.192.9.190	80	8/13/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.				
CVE-2011-4576	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.				
CVE-2014-0195	2.192.9.190	80	6/5/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.				
CVE-2014-3506	2.192.9.190	80	8/13/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.				
CVE-2014-3507	2.192.9.190	80	8/13/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.				
CVE-2014-0221	2.192.9.190	80	6/5/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.				
CVE-2014-3570	2.192.9.190	80	1/9/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.				
CVE-2012-0031	2.192.9.190	80	1/18/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.				
CVE-2018-1312	2.192.9.190	80	3/26/2018, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.				
CVE-2014-3508	2.192.9.190	80	8/13/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.				
CVE-2016-0704	2.192.9.190	80	3/2/2016, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2015-0288	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2012-2333	2.192.9.190	80	5/14/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.				
CVE-2015-1791	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.				
CVE-2014-3505	2.192.9.190	80	8/13/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.				
CVE-2015-1792	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.				
CVE-2015-1790	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.				
CVE-2015-0289	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.				
CVE-2014-3572	2.192.9.190	80	1/9/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.				
CVE-2016-0703	2.192.9.190	80	3/2/2016, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.				
CVE-2012-0884	2.192.9.190	80	3/13/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.				
CVE-2016-8743	2.192.9.190	80	7/27/2017, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.				
CVE-2011-0014	2.192.9.190	80	2/19/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka "OCSP stapling vulnerability."				
CVE-2010-0433	2.192.9.190	80	3/5/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.				
CVE-2016-5387	2.192.9.190	80	7/19/2016, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.				
CVE-2016-4975	2.192.9.190	80	8/14/2018, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).				
CVE-2015-1789	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.				
CVE-2012-0027	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.				
CVE-2010-0740	2.192.9.190	80	3/26/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.				
CVE-2019-20372	2.192.4.71	80	1/9/2020, 12:00:00 AM	2/10/2022, 9:57:17 AM
Vulnerability Description : NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.				
CVE-2017-7529	2.192.4.71	80	7/13/2017, 12:00:00 AM	2/10/2022, 9:57:17 AM
Vulnerability Description : Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.				
CVE-2018-16845	2.192.4.71	80	11/7/2018, 12:00:00 AM	2/10/2022, 9:57:17 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.				
CVE-2016-10708	2.192.4.184	22	1/21/2018, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2018-15919	2.192.4.184	22	8/28/2018, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6110	2.192.4.184	22	1/31/2019, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2020-14145	2.192.4.184	22	6/29/2020, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-10010	2.192.4.184	22	1/4/2017, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2018-15473	2.192.4.184	22	8/17/2018, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6109	2.192.4.184	22	1/31/2019, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2017-15906	2.192.4.184	22	10/26/2017, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6111	2.192.4.184	22	1/31/2019, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2010-5107	2.192.4.252	22	3/7/2013, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2016-0778	2.192.4.252	22	1/14/2016, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2020-14145	2.192.4.252	22	6/29/2020, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2017-15906	2.192.4.252	22	10/26/2017, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2016-0777	2.192.4.252	22	4/1/2016, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2018-15919	2.192.4.252	22	8/28/2018, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6111	2.192.4.221	22	1/31/2019, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2016-10010	2.192.4.221	22	1/4/2017, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.				
CVE-2019-6110	2.192.4.221	22	1/31/2019, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2017-15906	2.192.4.221	22	10/26/2017, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2018-15919	2.192.4.221	22	8/28/2018, 12:00:00 AM	2/8/2022, 10:15:59 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2016-10708	2.192.4.221	22	1/21/2018, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.				
CVE-2018-15473	2.192.4.221	22	8/17/2018, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2019-6109	2.192.4.221	22	1/31/2019, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				
CVE-2020-14145	2.192.4.221	22	6/29/2020, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2020-14145	2.192.6.117	22	6/29/2020, 12:00:00 AM	2/8/2022, 8:04:21 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2020-15778	2.192.6.117	22	7/24/2020, 12:00:00 AM	2/8/2022, 8:04:21 AM
Vulnerability Description : ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."				
CVE-2020-12062	2.192.6.117	22	6/1/2020, 12:00:00 AM	2/8/2022, 8:04:21 AM
Vulnerability Description : ** DISPUTED ** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not fail under normal circumstances."				
CVE-2014-2653	2.192.11.227	22	3/27/2014, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.				
CVE-2017-15906	2.192.11.227	22	10/26/2017, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2010-5107	2.192.11.227	22	3/7/2013, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.				
CVE-2020-14145	2.192.11.227	22	6/29/2020, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2016-0777	2.192.11.227	22	4/1/2016, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.				
CVE-2016-0778	2.192.11.227	22	1/14/2016, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.				
CVE-2014-2532	2.192.11.227	22	3/18/2014, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.				
CVE-2015-5352	2.192.11.227	22	8/3/2015, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.				
CVE-2015-6564	2.192.11.227	22	8/24/2015, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.				
CVE-2018-15919	2.192.11.227	22	8/28/2018, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2018-15919	2.192.8.230	22	8/28/2018, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'				
CVE-2019-6110	2.192.8.230	22	1/31/2019, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.				
CVE-2018-15473	2.192.8.230	22	8/17/2018, 12:00:00 AM	2/7/2022, 11:56:47 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.				
CVE-2020-14145	2.192.8.230	22	6/29/2020, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.				
CVE-2019-6111	2.192.8.230	22	1/31/2019, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).				
CVE-2017-15906	2.192.8.230	22	10/26/2017, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.				
CVE-2019-6109	2.192.8.230	22	1/31/2019, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.				

High-Severity Vulnerability in Last Observation

-0.8 SCORE IMPACT

We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.

Description

Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability.
Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

Recommendation

Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

143 findings

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8858	2.192.2.247	22	12/9/2016, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10012	2.192.2.247	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.2.247	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.2.167	22	12/9/2016, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10012	2.192.2.167	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.2.167	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2014-1692	2.192.2.120	22	1/29/2014, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.2.120	22	8/3/2015, 12:00:00 AM	3/8/2022, 6:04:00 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.2.119	22	1/29/2014, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.2.119	22	8/3/2015, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2017-9078	2.192.4.253	22	5/19/2017, 12:00:00 AM	3/8/2022, 5:30:10 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2015-5600	2.192.4.31	22	8/3/2015, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.4.31	22	1/29/2014, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2017-9078	2.192.0.211	22	5/19/2017, 12:00:00 AM	3/8/2022, 2:07:03 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2015-5600	2.192.5.95	22	8/3/2015, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.5.95	22	1/29/2014, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2017-9078	2.192.9.41	22	5/19/2017, 12:00:00 AM	3/7/2022, 11:14:16 PM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2014-1692	2.192.9.114	22	1/29/2014, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.9.114	22	8/3/2015, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2007-1718	2.192.0.124	8080	3/28/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : CRLF injection vulnerability in the mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows remote attackers to inject arbitrary e-mail headers and possibly conduct spam attacks via a control character immediately following folding of the (1) Subject or (2) To parameter, as demonstrated by a parameter containing a "\r\n\t\n" sequence, related to an increment bug in the SKIP_LONG_HEADER_SEP macro.				
CVE-2007-1890	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the msg_receive function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1, on FreeBSD and possibly other platforms, allows context-dependent attackers to execute arbitrary code via certain maxsize values, as demonstrated by 0xffffffff.				
CVE-2007-4658	2.192.0.124	8080	9/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The money_format function in PHP 5 before 5.2.4, and PHP 4 before 4.4.8, permits multiple (1) %i and (2) %n tokens, which has unknown impact and attack vectors, possibly related to a format string vulnerability.				
CVE-2011-3192	2.192.0.124	8080	8/29/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2007-0906	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple buffer overflows in PHP before 5.2.1 allow attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors in the (1) session, (2) zip, (3) imap, and (4) sqlite extensions; (5) stream filters; and the (6) str_replace, (7) mail, (8) ibase_delete_user, (9) ibase_add_user, and (10) ibase_modify_user functions. NOTE: vector 6 might actually be an integer overflow (CVE-2007-1885). NOTE: as of 20070411, vector (3) might involve the imap_mail_compose function (CVE-2007-1825).				
CVE-2009-3291	2.192.0.124	8080	9/22/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2008-3658	2.192.0.124	8080	8/15/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2007-4657	2.192.0.124	8080	9/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple integer overflows in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to obtain sensitive information (memory contents) or cause a denial of service (thread crash) via a large len value to the (1) strspn or (2) strcspn function, which triggers an out-of-bounds read. NOTE: this affects different product versions than CVE-2007-3996.				
CVE-2007-1883	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows context-dependent attackers to read arbitrary memory locations via an interruption that triggers a user space error handler that changes a parameter to an arbitrary pointer, as demonstrated via the iptcembed function, which calls certain convert_to_* functions with its input parameters.				
CVE-2011-1148	2.192.0.124	8080	3/18/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.				
CVE-2008-5557	2.192.0.124	8080	12/23/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2007-1888	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the sqlite_decode_binary function in src/encode.c in SQLite 2, as used by PHP 4.x through 5.x and other applications, allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter. NOTE: some PHP installations use a bundled version of sqlite without this vulnerability. The SQLite developer has argued that this issue could be due to a misuse of the sqlite_decode_binary() API.				
CVE-2009-4018	2.192.0.124	8080	11/29/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2008-2107	2.192.0.124	8080	5/7/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the rand and mt_rand functions and possibly bypass protection mechanisms that rely on an unknown initial seed.				
CVE-2012-2311	2.192.0.124	8080	5/11/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2011-3268	2.192.0.124	8080	8/25/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2007-3997	2.192.0.124	8080	9/4/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The (1) MySQL and (2) MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INFILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.				
CVE-2009-3293	2.192.0.124	8080	9/22/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2011-1092	2.192.0.124	8080	3/15/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2007-0905	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.2.1 allows attackers to bypass safe_mode and open_basedir restrictions via unspecified vectors in the session extension. NOTE: it is possible that this issue is a duplicate of CVE-2006-6383.				
CVE-2011-1153	2.192.0.124	8080	3/16/2011, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2007-1887	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the sqlite_decode_binary function in the bundled sqlite library in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter, as demonstrated by calling the sqlite_udf_decode_binary function with a 0x01 character.				
CVE-2007-1825	2.192.0.124	8080	4/2/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the imap_mail_compose function in PHP 5 before 5.2.1, and PHP 4 before 4.4.5, allows remote attackers to execute arbitrary code via a long boundary string in a type.parameters field. NOTE: as of 20070411, it appears that this issue might be subsumed by CVE-2007-0906.3.				
CVE-2007-1461	2.192.0.124	8080	3/14/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The compress.bzip2:// URL wrapper provided by the bz2 extension in PHP before 4.4.7, and 5.x before 5.2.2, does not implement safemode or open_basedir checks, which allows remote attackers to read bzip2 archives located outside of the intended directories.				
CVE-2009-3292	2.192.0.124	8080	9/22/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2007-1376	2.192.0.124	8080	3/10/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The shmop functions in PHP before 4.4.5, and before 5.2.1 in the 5.x series, do not verify that their arguments correspond to a shmop resource, which allows context-dependent attackers to read and write arbitrary memory locations via arguments associated with an inappropriate resource, as demonstrated by a GD Image resource.				
CVE-2007-1700	2.192.0.124	8080	3/27/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The session extension in PHP 4 before 4.4.5, and PHP 5 before 5.2.1, calculates the reference count for the session variables without considering the internal pointer from the session globals, which allows context-dependent attackers to execute arbitrary code via a crafted string in the session_register after unsetting HTTP_SESSION_VARS and _SESSION, which destroys the session data Hashtable.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2012-2386	2.192.0.124	8080	7/7/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2007-2844	2.192.0.124	8080	5/24/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4.x and 5.x before 5.2.1, when running on multi-threaded systems, does not ensure thread safety for libc crypt function calls using protection schemes such as a mutex, which creates race conditions that allow remote attackers to overwrite internal program memory and gain system access.				
CVE-2008-2108	2.192.0.124	8080	5/7/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.				
CVE-2007-1885	2.192.0.124	8080	4/6/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the str_replace function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via a single character search string in conjunction with a long replacement string, which overflows a 32 bit length counter. NOTE: this is probably the same issue as CVE-2007-0906.6.				
CVE-2007-1864	2.192.0.124	8080	5/9/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the bundled libxmlrpc library in PHP before 4.4.7, and 5.x before 5.2.2, has unknown impact and remote attack vectors.				
CVE-2007-2511	2.192.0.124	8080	5/9/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Buffer overflow in the user_filter_factory_create function in PHP before 5.2.2 has unknown impact and local attack vectors.				
CVE-2007-0909	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Multiple format string vulnerabilities in PHP before 5.2.1 might allow attackers to execute arbitrary code via format string specifiers to (1) all of the *print functions on 64-bit systems, and (2) the odbc_result_all function.				
CVE-2013-1635	2.192.0.124	8080	3/6/2013, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2008-0145	2.192.0.124	8080	1/8/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in glob in PHP before 4.4.8, when open_basedir is enabled, has unknown impact and attack vectors. NOTE: this issue reportedly exists because of a regression related to CVE-2007-4663.				
CVE-2009-4143	2.192.0.124	8080	12/21/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2007-1777	2.192.0.124	8080	3/30/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Integer overflow in the zip_read_entry function in PHP 4 before 4.4.5 allows remote attackers to execute arbitrary code via a ZIP archive that contains an entry with a length value of 0xffffffff, which is incremented before use in an emalloc call, triggering a heap overflow.				
CVE-2007-0910	2.192.0.124	8080	2/13/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.1 allows attackers to "clobber" certain super-global variables via unspecified vectors.				
CVE-2012-2688	2.192.0.124	8080	7/20/2012, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2014-9427	2.192.0.124	8080	1/3/2015, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2017-9078	2.192.2.149	22	5/19/2017, 12:00:00 AM	2/24/2022, 3:11:37 PM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-3167	2.192.5.76	80	6/20/2017, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.				
CVE-2017-7679	2.192.5.76	80	6/20/2017, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2018-16844	2.192.3.32	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:53:59 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.3.32	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:53:59 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2017-7679	2.192.3.142	80	6/20/2017, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2010-2225	2.192.3.142	80	6/24/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.				
CVE-2012-2688	2.192.3.142	80	7/20/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2008-3658	2.192.3.142	80	8/15/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2008-2050	2.192.3.142	80	5/5/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2012-2110	2.192.3.142	80	4/19/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2012-1823	2.192.3.142	80	5/11/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.				
CVE-2008-5624	2.192.3.142	80	12/17/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.				
CVE-2009-4143	2.192.3.142	80	12/21/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2010-1868	2.192.3.142	80	5/7/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.				
CVE-2009-3291	2.192.3.142	80	9/22/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2009-4018	2.192.3.142	80	11/29/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2011-3192	2.192.3.142	80	8/29/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2009-3293	2.192.3.142	80	9/22/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2008-0599	2.192.3.142	80	5/5/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.				
CVE-2008-5557	2.192.3.142	80	12/23/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2008-5658	2.192.3.142	80	12/17/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.				
CVE-2007-1581	2.192.3.142	80	3/21/2007, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.				
CVE-2014-8176	2.192.3.142	80	6/12/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2008-7002	2.192.3.142	80	8/19/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.				
CVE-2014-9427	2.192.3.142	80	1/3/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2012-2386	2.192.3.142	80	7/7/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2008-2051	2.192.3.142	80	5/5/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."				
CVE-2013-1635	2.192.3.142	80	3/6/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2009-3245	2.192.3.142	80	3/5/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.				
CVE-2014-8626	2.192.3.142	80	11/23/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.				
CVE-2012-2311	2.192.3.142	80	5/11/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2011-1153	2.192.3.142	80	3/16/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2010-1129	2.192.3.142	80	3/26/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.				
CVE-2010-3864	2.192.3.142	80	11/17/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2008-5625	2.192.3.142	80	12/17/2008, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.				
CVE-2009-3292	2.192.3.142	80	9/22/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2010-0742	2.192.3.142	80	6/3/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2011-1092	2.192.3.142	80	3/15/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2011-4109	2.192.3.142	80	1/6/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2015-0292	2.192.3.142	80	3/19/2015, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2010-4252	2.192.3.142	80	12/6/2010, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2014-3567	2.192.3.142	80	10/19/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2011-3268	2.192.3.142	80	8/25/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2018-16843	2.192.3.235	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:49:40 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.3.235	80	11/7/2018, 12:00:00 AM	2/11/2022, 8:49:40 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.4.54	80	11/7/2018, 12:00:00 AM	2/11/2022, 1:43:31 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.4.54	80	11/7/2018, 12:00:00 AM	2/11/2022, 1:43:31 PM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2019-9020	2.192.3.2	80	2/22/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.				
CVE-2018-12882	2.192.3.2	80	6/26/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.				
CVE-2019-9023	2.192.3.2	80	2/22/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.				
CVE-2019-9021	2.192.3.2	80	2/22/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.				
CVE-2018-19518	2.192.3.2	80	11/25/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.				
CVE-2019-9641	2.192.3.2	80	3/9/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.				
CVE-2019-11043	2.192.3.2	80	10/28/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.				
CVE-2019-0211	2.192.3.2	80	4/8/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.				
CVE-2018-16843	2.192.2.24	80	11/7/2018, 12:00:00 AM	2/11/2022, 2:25:44 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.2.24	80	11/7/2018, 12:00:00 AM	2/11/2022, 2:25:44 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2010-4252	2.192.9.190	80	12/6/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2015-0292	2.192.9.190	80	3/19/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2014-8176	2.192.9.190	80	6/12/2015, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2010-3864	2.192.9.190	80	11/17/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2011-3192	2.192.9.190	80	8/29/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2011-4109	2.192.9.190	80	1/6/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2017-3167	2.192.9.190	80	6/20/2017, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.				
CVE-2017-3169	2.192.9.190	80	6/20/2017, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.				
CVE-2010-0742	2.192.9.190	80	6/3/2010, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2012-2110	2.192.9.190	80	4/19/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2014-3567	2.192.9.190	80	10/19/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2017-7679	2.192.9.190	80	6/20/2017, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2018-16844	2.192.4.71	80	11/7/2018, 12:00:00 AM	2/10/2022, 9:57:17 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.4.71	80	11/7/2018, 12:00:00 AM	2/10/2022, 9:57:17 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-10012	2.192.4.184	22	1/4/2017, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.4.184	22	1/4/2017, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.4.184	22	12/9/2016, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2017-9078	2.192.5.21	22	5/19/2017, 12:00:00 AM	2/8/2022, 3:34:29 PM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2016-10012	2.192.4.221	22	1/4/2017, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.4.221	22	1/4/2017, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.4.221	22	12/9/2016, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2014-1692	2.192.11.227	22	1/29/2014, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.11.227	22	8/3/2015, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2017-9078	2.192.10.212	22	5/19/2017, 12:00:00 AM	2/8/2022, 5:14:23 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-9078	2.192.1.53	22	5/19/2017, 12:00:00 AM	2/8/2022, 12:42:06 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				

Medium-severity CVE patching analyzed

This analysis reflects the number of medium-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.

Description

We analyze patching coverage for medium-severity Common Vulnerabilities and Exposures (CVEs). We base this analysis on the number and percentage of medium-severity vulnerabilities that were resolved on the network since their detection, and the average resolution time over a 180-day period. Medium-severity CVEs have a Common Vulnerability Scoring System (CVSS v2) base score that ranges between 4.0 and 6.9. While high-severity vulnerabilities may warrant more urgent attention, maintaining a regular patching cadence for all vulnerabilities is an important security best practice. See metrics in the table below, including the number of vulnerabilities resolved in different time windows ranging less than 60 days to over 180.

Recommendation

Monitor CVE lists and vulnerability repositories for exploit code that may affect the network infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.

1 finding

ALL ACTIVE IN PAST 180 DAYS	RESOLVED ISSUES	RESOLVED %	AVERAGE DAYS TO RESOLVE	RESOLVED: 60 DAYS OR LESS	RESOLVED: 60-120 DAYS	RESOLVED: 121-180 DAYS	RESOLVED: OVER 180 DAYS	LAST UPDATE

ALL ACTIVE IN PAST 180 DAYS	RESOLVED ISSUES	RESOLVED %	AVERAGE DAYS TO RESOLVE	RESOLVED: 60 DAYS OR LESS	RESOLVED: 60-120 DAYS	RESOLVED: 121-180 DAYS	RESOLVED: OVER 180 DAYS	LAST UPDATE
1340	840	63	45	830	10			3/13/2022, 12:00:00 AM

High Severity CVEs Patching Cadence

-1.1 SCORE IMPACT

High severity vulnerability seen on network more than 45 days after CVE was published.

Description
Based on scan data, the company had high severity CVE vulnerability that was open longer than 45 days after the CVE was published. High severity CVEs are those with a documented CVSS severity over 7.0. It is best practice in standards such as PCI DSS to mitigate or patch high severity vulnerabilities within 45 days. Details on each vulnerability are listed in the table below.

Recommendation
Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all software and hardware in use within your enterprise, ensuring that all the latest patches are implemented as they are released.

319 findings

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-8858	2.192.2.247	22	3/8/2022, 11:42:35 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10009	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-10012	2.192.2.247	22	3/8/2022, 11:42:35 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-8858	2.192.2.167	22	3/8/2022, 11:42:27 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10012	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.2.167	22	3/8/2022, 11:42:27 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2015-5600	2.192.2.120	22	3/8/2022, 6:04:00 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.2.120	22	3/8/2022, 6:04:00 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2014-1692	2.192.2.119	22	3/8/2022, 6:02:46 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.2.119	22	3/8/2022, 6:02:46 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2017-9078	2.192.4.253	22	3/8/2022, 5:30:10 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2015-5600	2.192.4.31	22	3/8/2022, 5:28:55 AM	8/3/2015, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.4.31	22	3/8/2022, 5:28:55 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2017-9078	2.192.0.211	22	3/8/2022, 2:07:03 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2014-1692	2.192.5.95	22	3/8/2022, 12:55:13 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.5.95	22	3/8/2022, 12:55:13 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2017-9078	2.192.9.41	22	3/7/2022, 11:14:16 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2015-5600	2.192.9.114	22	3/7/2022, 11:12:49 PM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.9.114	22	3/7/2022, 11:12:49 PM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2009-4018	2.192.0.124	8080	2/27/2022, 8:38:21 PM	11/29/2009, 12:00:00 AM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2007-1718	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/28/2007, 12:00:00 AM
Vulnerability Description : CRLF injection vulnerability in the mail function in PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows remote attackers to inject arbitrary e-mail headers and possibly conduct spam attacks via a control character immediately following folding of the (1) Subject or (2) To parameter, as demonstrated by a parameter containing a "\r\n\t\n" sequence, related to an increment bug in the SKIP_LONG_HEADER_SEP macro.				
CVE-2013-1635	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2008-2107	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/7/2008, 12:00:00 AM
Vulnerability Description : The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 32-bit systems, performs a multiplication using values that can produce a zero seed in rare circumstances, which allows context-dependent attackers to predict subsequent values of the rand and mt_rand functions and possibly bypass protection mechanisms that rely on an unknown initial seed.				
CVE-2007-1887	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the sqlite_decode_binary function in the bundled sqlite library in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter, as demonstrated by calling the sqlite_udf_decode_binary function with a 0x01 character.				
CVE-2007-0906	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in PHP before 5.2.1 allow attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors in the (1) session, (2) zip, (3) imap, and (4) sqlite extensions; (5) stream filters; and the (6) str_replace, (7) mail, (8) ibase_delete_user, (9) ibase_add_user, and (10) ibase_modify_user functions. NOTE: vector 6 might actually be an integer overflow (CVE-2007-1885). NOTE: as of 20070411, vector (3) might involve the imap_mail_compose function (CVE-2007-1825).				
CVE-2012-2688	2.192.0.124	8080	2/27/2022, 8:38:21 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2011-1153	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/16/2011, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2012-2311	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2007-1888	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the sqlite_decode_binary function in src/encode.c in SQLite 2, as used by PHP 4.x through 5.x and other applications, allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter. NOTE: some PHP installations use a bundled version of sqlite without this vulnerability. The SQLite developer has argued that this issue could be due to a misuse of the sqlite_decode_binary() API.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2007-0905	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : PHP before 5.2.1 allows attackers to bypass safe_mode and open_basedir restrictions via unspecified vectors in the session extension. NOTE: it is possible that this issue is a duplicate of CVE-2006-6383.				
CVE-2011-1092	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/15/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2007-4658	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/4/2007, 12:00:00 AM
Vulnerability Description : The money_format function in PHP 5 before 5.2.4, and PHP 4 before 4.4.8, permits multiple (1) %i and (2) %n tokens, which has unknown impact and attack vectors, possibly related to a format string vulnerability.				
CVE-2008-2108	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/7/2008, 12:00:00 AM
Vulnerability Description : The GENERATE_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt_rand functions.				
CVE-2007-1885	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Integer overflow in the str_replace function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via a single character search string in conjunction with a long replacement string, which overflows a 32 bit length counter. NOTE: this is probably the same issue as CVE-2007-0906.6.				
CVE-2011-3268	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2007-0909	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in PHP before 5.2.1 might allow attackers to execute arbitrary code via format string specifiers to (1) all of the *print functions on 64-bit systems, and (2) the odbc_result_all function.				
CVE-2007-3997	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/4/2007, 12:00:00 AM
Vulnerability Description : The (1) MySQL and (2) MySQLi extensions in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to bypass safe_mode and open_basedir restrictions via MySQL LOCAL INFILE operations, as demonstrated by a query with LOAD DATA LOCAL INFILE.				
CVE-2008-3658	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2011-1148	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/18/2011, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.				
CVE-2014-9427	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/3/2015, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2007-2511	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/9/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the user_filter_factory_create function in PHP before 5.2.2 has unknown impact and local attack vectors.				
CVE-2007-1864	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/9/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the bundled libxmlrpc library in PHP before 4.4.7, and 5.x before 5.2.2, has unknown impact and remote attack vectors.				
CVE-2007-1890	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : Integer overflow in the msg_receive function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1, on FreeBSD and possibly other platforms, allows context-dependent attackers to execute arbitrary code via certain maxsize values, as demonstrated by 0xffffffff.				
CVE-2007-1825	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/2/2007, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imap_mail_compose function in PHP 5 before 5.2.1, and PHP 4 before 4.4.5, allows remote attackers to execute arbitrary code via a long boundary string in a type.parameters field. NOTE: as of 20070411, it appears that this issue might be subsumed by CVE-2007-0906.3.				
CVE-2007-1883	2.192.0.124	8080	2/27/2022, 8:38:21 PM	4/6/2007, 12:00:00 AM
Vulnerability Description : PHP 4.0.0 through 4.4.6 and 5.0.0 through 5.2.1 allows context-dependent attackers to read arbitrary memory locations via an interruption that triggers a user space error handler that changes a parameter to an arbitrary pointer, as demonstrated via the iptcembed function, which calls certain convert_to_* functions with its input parameters.				
CVE-2007-2844	2.192.0.124	8080	2/27/2022, 8:38:21 PM	5/24/2007, 12:00:00 AM
Vulnerability Description : PHP 4.x and 5.x before 5.2.1, when running on multi-threaded systems, does not ensure thread safety for libc crypt function calls using protection schemes such as a mutex, which creates race conditions that allow remote attackers to overwrite internal program memory and gain system access.				
CVE-2012-2386	2.192.0.124	8080	2/27/2022, 8:38:21 PM	7/7/2012, 12:00:00 AM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2007-1376	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/10/2007, 12:00:00 AM
Vulnerability Description : The shmop functions in PHP before 4.4.5, and before 5.2.1 in the 5.x series, do not verify that their arguments correspond to a shmop resource, which allows context-dependent attackers to read and write arbitrary memory locations via arguments associated with an inappropriate resource, as demonstrated by a GD Image resource.				
CVE-2008-0145	2.192.0.124	8080	2/27/2022, 8:38:21 PM	1/8/2008, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in glob in PHP before 4.4.8, when open_basedir is enabled, has unknown impact and attack vectors. NOTE: this issue reportedly exists because of a regression related to CVE-2007-4663.				
CVE-2009-3293	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2007-1700	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/27/2007, 12:00:00 AM
Vulnerability Description : The session extension in PHP 4 before 4.4.5, and PHP 5 before 5.2.1, calculates the reference count for the session variables without considering the internal pointer from the session globals, which allows context-dependent attackers to execute arbitrary code via a crafted string in the session_register after unsetting HTTP_SESSION_VARS and _SESSION, which destroys the session data Hashtable.				
CVE-2009-3291	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/22/2009, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2011-3192	2.192.0.124	8080	2/27/2022, 8:38:21 PM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2007-0910	2.192.0.124	8080	2/27/2022, 8:38:21 PM	2/13/2007, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.1 allows attackers to "clobber" certain super-global variables via unspecified vectors.				
CVE-2007-1777	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/30/2007, 12:00:00 AM
Vulnerability Description : Integer overflow in the zip_read_entry function in PHP 4 before 4.4.5 allows remote attackers to execute arbitrary code via a ZIP archive that contains an entry with a length value of 0xffffffff, which is incremented before use in an emalloc call, triggering a heap overflow.				
CVE-2009-3292	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2008-5557	2.192.0.124	8080	2/27/2022, 8:38:21 PM	12/23/2008, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2009-4143	2.192.0.124	8080	2/27/2022, 8:38:21 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2007-1461	2.192.0.124	8080	2/27/2022, 8:38:21 PM	3/14/2007, 12:00:00 AM
Vulnerability Description : The compress.bzip2:// URL wrapper provided by the bz2 extension in PHP before 4.4.7, and 5.x before 5.2.2, does not implement safemode or open_basedir checks, which allows remote attackers to read bzip2 archives located outside of the intended directories.				
CVE-2007-4657	2.192.0.124	8080	2/27/2022, 8:38:21 PM	9/4/2007, 12:00:00 AM
Vulnerability Description : Multiple integer overflows in PHP 4 before 4.4.8, and PHP 5 before 5.2.4, allow remote attackers to obtain sensitive information (memory contents) or cause a denial of service (thread crash) via a large len value to the (1) strspn or (2) strcspn function, which triggers an out-of-bounds read. NOTE: this affects different product versions than CVE-2007-3996.				
CVE-2017-9078	2.192.2.149	22	2/24/2022, 3:11:37 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-3167	2.192.5.76	80	2/12/2022, 4:34:44 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.				
CVE-2017-7679	2.192.5.76	80	2/12/2022, 4:34:44 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2018-16844	2.192.3.32	80	2/11/2022, 8:53:59 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.3.32	80	2/11/2022, 8:53:59 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2014-3567	2.192.3.142	80	2/11/2022, 8:52:12 PM	10/19/2014, 12:00:00 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2015-0292	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2009-4018	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/29/2009, 12:00:00 AM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2010-3864	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/17/2010, 12:00:00 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2014-8626	2.192.3.142	80	2/11/2022, 8:52:12 PM	11/23/2014, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.				
CVE-2010-0742	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/3/2010, 12:00:00 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2008-5624	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.				
CVE-2009-3292	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2010-2225	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/24/2010, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.				
CVE-2009-3245	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/5/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.				
CVE-2008-2051	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."				
CVE-2007-1581	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/21/2007, 12:00:00 AM
Vulnerability Description : The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.				
CVE-2011-3192	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2011-4109	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2014-9427	2.192.3.142	80	2/11/2022, 8:52:12 PM	1/3/2015, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2008-5557	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/23/2008, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2011-3268	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2017-7679	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2009-3291	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2008-3658	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2011-1092	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/15/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2012-2110	2.192.3.142	80	2/11/2022, 8:52:12 PM	4/19/2012, 12:00:00 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2012-2688	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2008-0599	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.				
CVE-2012-2311	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2008-7002	2.192.3.142	80	2/11/2022, 8:52:12 PM	8/19/2009, 12:00:00 AM
Vulnerability Description : PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.				
CVE-2014-8176	2.192.3.142	80	2/11/2022, 8:52:12 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2008-5658	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.				
CVE-2012-2386	2.192.3.142	80	2/11/2022, 8:52:12 PM	7/7/2012, 12:00:00 AM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2011-1153	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/16/2011, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2008-5625	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.				
CVE-2013-1635	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2009-3293	2.192.3.142	80	2/11/2022, 8:52:12 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2009-4143	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2010-1129	2.192.3.142	80	2/11/2022, 8:52:12 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.				
CVE-2010-1868	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.				
CVE-2010-4252	2.192.3.142	80	2/11/2022, 8:52:12 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2012-1823	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.				
CVE-2008-2050	2.192.3.142	80	2/11/2022, 8:52:12 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.				
CVE-2018-16844	2.192.3.235	80	2/11/2022, 8:49:40 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.3.235	80	2/11/2022, 8:49:40 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.4.54	80	2/11/2022, 1:43:31 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.4.54	80	2/11/2022, 1:43:31 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-12882	2.192.3.2	80	2/11/2022, 2:44:31 AM	6/26/2018, 12:00:00 AM
Vulnerability Description : exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.				
CVE-2019-0211	2.192.3.2	80	2/11/2022, 2:44:31 AM	4/8/2019, 12:00:00 AM
Vulnerability Description : In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.				
CVE-2018-19518	2.192.3.2	80	2/11/2022, 2:44:31 AM	11/25/2018, 12:00:00 AM
Vulnerability Description : University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.				
CVE-2019-9021	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.				
CVE-2019-9020	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.				
CVE-2019-9641	2.192.3.2	80	2/11/2022, 2:44:31 AM	3/9/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.				
CVE-2019-9023	2.192.3.2	80	2/11/2022, 2:44:31 AM	2/22/2019, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.				
CVE-2019-11043	2.192.3.2	80	2/11/2022, 2:44:31 AM	10/28/2019, 12:00:00 AM
Vulnerability Description : In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.				
CVE-2018-16844	2.192.2.24	80	2/11/2022, 2:25:44 AM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.2.24	80	2/11/2022, 2:25:44 AM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2014-3567	2.192.9.190	80	2/10/2022, 11:59:49 AM	10/19/2014, 12:00:00 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2010-3864	2.192.9.190	80	2/10/2022, 11:59:49 AM	11/17/2010, 12:00:00 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2017-3167	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.				
CVE-2014-8176	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2011-3192	2.192.9.190	80	2/10/2022, 11:59:49 AM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2010-4252	2.192.9.190	80	2/10/2022, 11:59:49 AM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2011-4109	2.192.9.190	80	2/10/2022, 11:59:49 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2017-3169	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.				
CVE-2010-0742	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/3/2010, 12:00:00 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2017-7679	2.192.9.190	80	2/10/2022, 11:59:49 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2015-0292	2.192.9.190	80	2/10/2022, 11:59:49 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2012-2110	2.192.9.190	80	2/10/2022, 11:59:49 AM	4/19/2012, 12:00:00 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2018-16843	2.192.4.71	80	2/10/2022, 9:57:17 AM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.4.71	80	2/10/2022, 9:57:17 AM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2016-10012	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-8858	2.192.4.184	22	2/8/2022, 3:36:45 PM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10009	2.192.4.184	22	2/8/2022, 3:36:45 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2017-9078	2.192.5.21	22	2/8/2022, 3:34:29 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2016-10012	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.4.221	22	2/8/2022, 10:15:59 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.4.221	22	2/8/2022, 10:15:59 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2015-5600	2.192.11.227	22	2/8/2022, 7:40:14 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.11.227	22	2/8/2022, 7:40:14 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2017-9078	2.192.10.212	22	2/8/2022, 5:14:23 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-9078	2.192.1.53	22	2/8/2022, 12:42:06 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2010-4478	2.192.9.81	2222	1/15/2022, 11:15:32 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				
CVE-2016-10009	2.192.5.195	22	1/15/2022, 1:33:16 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-10012	2.192.5.195	22	1/15/2022, 1:33:16 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-8858	2.192.5.195	22	1/15/2022, 1:33:16 PM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2010-4478	2.192.8.82	2222	1/14/2022, 9:29:32 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				
CVE-2017-9078	2.192.6.176	22	1/14/2022, 6:10:21 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-9078	2.192.6.169	222	1/14/2022, 5:06:25 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2013-4547	2.192.3.101	443	1/14/2022, 3:39:11 PM	11/23/2013, 12:00:00 AM
Vulnerability Description : nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.				
CVE-2018-16843	2.192.3.101	443	1/14/2022, 3:39:11 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2013-0337	2.192.3.101	443	1/14/2022, 3:39:11 PM	10/27/2013, 12:00:00 AM
Vulnerability Description : The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.				
CVE-2016-0746	2.192.3.101	443	1/14/2022, 3:39:11 PM	2/15/2016, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the resolver in nginx 0.6.18 through 1.8.0 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.				
CVE-2018-16844	2.192.3.101	443	1/14/2022, 3:39:11 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2017-9078	2.192.14.215	22	1/13/2022, 5:22:26 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2018-16843	2.192.2.138	80	1/10/2022, 9:09:18 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.2.138	80	1/10/2022, 9:09:18 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16844	2.192.2.171	80	1/10/2022, 9:09:14 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2018-16843	2.192.2.171	80	1/10/2022, 9:09:14 PM	11/7/2018, 12:00:00 AM
Vulnerability Description : nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.				
CVE-2008-2050	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.				
CVE-2007-1581	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/21/2007, 12:00:00 AM
Vulnerability Description : The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.				
CVE-2010-1868	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.				
CVE-2012-2110	2.192.7.173	80	1/10/2022, 7:35:53 PM	4/19/2012, 12:00:00 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2010-1129	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.				
CVE-2009-3293	2.192.7.173	80	1/10/2022, 7:35:53 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2008-5624	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.				
CVE-2010-2225	2.192.7.173	80	1/10/2022, 7:35:53 PM	6/24/2010, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.				
CVE-2011-3192	2.192.7.173	80	1/10/2022, 7:35:53 PM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2014-9427	2.192.7.173	80	1/10/2022, 7:35:53 PM	1/3/2015, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2008-3658	2.192.7.173	80	1/10/2022, 7:35:53 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2009-3292	2.192.7.173	80	1/10/2022, 7:35:53 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2013-1635	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2010-4252	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2012-2386	2.192.7.173	80	1/10/2022, 7:35:53 PM	7/7/2012, 12:00:00 AM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2009-3291	2.192.7.173	80	1/10/2022, 7:35:53 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2012-1823	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.				
CVE-2008-7002	2.192.7.173	80	1/10/2022, 7:35:53 PM	8/19/2009, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.				
CVE-2011-1153	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/16/2011, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2014-8176	2.192.7.173	80	1/10/2022, 7:35:53 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2015-0292	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2011-3268	2.192.7.173	80	1/10/2022, 7:35:53 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2014-8626	2.192.7.173	80	1/10/2022, 7:35:53 PM	11/23/2014, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.				
CVE-2008-5658	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.				
CVE-2010-3864	2.192.7.173	80	1/10/2022, 7:35:53 PM	11/17/2010, 12:00:00 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2008-0599	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.				
CVE-2008-2051	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."				
CVE-2012-2311	2.192.7.173	80	1/10/2022, 7:35:53 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2008-5557	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/23/2008, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2012-2688	2.192.7.173	80	1/10/2022, 7:35:53 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2010-0742	2.192.7.173	80	1/10/2022, 7:35:53 PM	6/3/2010, 12:00:00 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2017-7679	2.192.7.173	80	1/10/2022, 7:35:53 PM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2011-1092	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/15/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2011-4109	2.192.7.173	80	1/10/2022, 7:35:53 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2009-4143	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2009-3245	2.192.7.173	80	1/10/2022, 7:35:53 PM	3/5/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.				
CVE-2014-3567	2.192.7.173	80	1/10/2022, 7:35:53 PM	10/19/2014, 12:00:00 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2008-5625	2.192.7.173	80	1/10/2022, 7:35:53 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.				
CVE-2009-4018	2.192.7.173	80	1/10/2022, 7:35:53 PM	11/29/2009, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2019-9023	2.192.3.85	80	1/10/2022, 6:33:04 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.				
CVE-2019-0211	2.192.3.85	80	1/10/2022, 6:33:04 AM	4/8/2019, 12:00:00 AM
Vulnerability Description : In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.				
CVE-2018-12882	2.192.3.85	80	1/10/2022, 6:33:04 AM	6/26/2018, 12:00:00 AM
Vulnerability Description : exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.				
CVE-2019-11043	2.192.3.85	80	1/10/2022, 6:33:04 AM	10/28/2019, 12:00:00 AM
Vulnerability Description : In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.				
CVE-2019-9641	2.192.3.85	80	1/10/2022, 6:33:04 AM	3/9/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.				
CVE-2018-19518	2.192.3.85	80	1/10/2022, 6:33:04 AM	11/25/2018, 12:00:00 AM
Vulnerability Description : University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.				
CVE-2019-9020	2.192.3.85	80	1/10/2022, 6:33:04 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.				
CVE-2019-9021	2.192.3.85	80	1/10/2022, 6:33:04 AM	2/22/2019, 12:00:00 AM
Vulnerability Description : An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.				
CVE-2012-2688	2.192.4.83	80	1/10/2022, 3:25:06 AM	7/20/2012, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2008-2050	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/5/2008, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.				
CVE-2010-4252	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2008-5557	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/23/2008, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2017-7679	2.192.4.83	80	1/10/2022, 3:25:06 AM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2009-4143	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/21/2009, 12:00:00 AM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2007-1581	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/21/2007, 12:00:00 AM
Vulnerability Description : The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.				
CVE-2014-8176	2.192.4.83	80	1/10/2022, 3:25:06 AM	6/12/2015, 12:00:00 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2011-1092	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/15/2011, 12:00:00 AM
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2015-0292	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/19/2015, 12:00:00 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2014-9427	2.192.4.83	80	1/10/2022, 3:25:06 AM	1/3/2015, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2011-1153	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/16/2011, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2010-1868	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/7/2010, 12:00:00 AM
Vulnerability Description : The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.				
CVE-2008-7002	2.192.4.83	80	1/10/2022, 3:25:06 AM	8/19/2009, 12:00:00 AM
Vulnerability Description : PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.				
CVE-2008-2051	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/5/2008, 12:00:00 AM
Vulnerability Description : The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."				
CVE-2014-3567	2.192.4.83	80	1/10/2022, 3:25:06 AM	10/19/2014, 12:00:00 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2008-5658	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/17/2008, 12:00:00 AM
Vulnerability Description : Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.				
CVE-2009-3292	2.192.4.83	80	1/10/2022, 3:25:06 AM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2008-5624	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.				
CVE-2010-3864	2.192.4.83	80	1/10/2022, 3:25:06 AM	11/17/2010, 12:00:00 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2009-3291	2.192.4.83	80	1/10/2022, 3:25:06 AM	9/22/2009, 12:00:00 AM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2010-1129	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/26/2010, 12:00:00 AM
Vulnerability Description : The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.				
CVE-2009-3245	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/5/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.				
CVE-2012-2386	2.192.4.83	80	1/10/2022, 3:25:06 AM	7/7/2012, 12:00:00 AM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2010-2225	2.192.4.83	80	1/10/2022, 3:25:06 AM	6/24/2010, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.				
CVE-2012-2311	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2014-8626	2.192.4.83	80	1/10/2022, 3:25:06 AM	11/23/2014, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.				
CVE-2009-4018	2.192.4.83	80	1/10/2022, 3:25:06 AM	11/29/2009, 12:00:00 AM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2011-3192	2.192.4.83	80	1/10/2022, 3:25:06 AM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2012-2110	2.192.4.83	80	1/10/2022, 3:25:06 AM	4/19/2012, 12:00:00 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2008-3658	2.192.4.83	80	1/10/2022, 3:25:06 AM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2013-1635	2.192.4.83	80	1/10/2022, 3:25:06 AM	3/6/2013, 12:00:00 AM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2011-4109	2.192.4.83	80	1/10/2022, 3:25:06 AM	1/6/2012, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2008-0599	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/5/2008, 12:00:00 AM
Vulnerability Description : The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.				
CVE-2010-0742	2.192.4.83	80	1/10/2022, 3:25:06 AM	6/3/2010, 12:00:00 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2008-5625	2.192.4.83	80	1/10/2022, 3:25:06 AM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.				
CVE-2012-1823	2.192.4.83	80	1/10/2022, 3:25:06 AM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.				
CVE-2011-3268	2.192.4.83	80	1/10/2022, 3:25:06 AM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2009-3293	2.192.4.83	80	1/10/2022, 3:25:06 AM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2017-14491	2.192.2.231	53	1/9/2022, 4:05:09 PM	10/3/2017, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.				
CVE-2016-10012	2.192.11.11	22	1/8/2022, 12:36:47 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-10009	2.192.11.11	22	1/8/2022, 12:36:47 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.11.11	22	1/8/2022, 12:36:47 PM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10009	2.192.8.21	22	1/8/2022, 11:40:31 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.8.21	22	1/8/2022, 11:40:31 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10012	2.192.8.21	22	1/8/2022, 11:40:31 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2017-9078	2.192.8.161	22	1/8/2022, 5:53:32 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2010-4478	2.192.2.231	22	1/8/2022, 5:31:38 AM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				
CVE-2017-9078	2.192.7.111	22	1/8/2022, 3:39:44 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-9078	2.192.5.128	22	1/8/2022, 12:32:20 AM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2017-9078	2.192.4.142	22	1/7/2022, 10:20:54 PM	5/19/2017, 12:00:00 AM
Vulnerability Description : The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.				
CVE-2014-1692	2.192.4.220	22	1/4/2022, 9:44:43 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-5600	2.192.4.220	22	1/4/2022, 9:44:43 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-3567	2.192.0.249	8000	12/25/2021, 8:23:06 PM	10/19/2014, 12:00:00 AM
Vulnerability Description : Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.				
CVE-2009-4143	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/21/2009, 12:00:00 AM
Vulnerability Description : PHP before 5.2.12 does not properly handle session data, which has unspecified impact and attack vectors related to (1) interrupt corruption of the SESSION superglobal array and (2) the session.save_path directive.				
CVE-2015-0292	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/19/2015, 12:00:00 AM
Vulnerability Description : Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.				
CVE-2008-2050	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.				
CVE-2010-3864	2.192.0.249	8000	12/25/2021, 8:23:06 PM	11/17/2010, 12:00:00 AM
Vulnerability Description : Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.				
CVE-2013-1635	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/6/2013, 12:00:00 AM
Vulnerability Description : ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.				
CVE-2007-1581	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/21/2007, 12:00:00 AM
Vulnerability Description : The resource system in PHP 5.0.0 through 5.2.1 allows context-dependent attackers to execute arbitrary code by interrupting the hash_update_file function via a userspace (1) error or (2) stream handler, which can then be used to destroy and modify internal resources. NOTE: it was later reported that PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 are also affected.				
CVE-2008-3658	2.192.0.249	8000	12/25/2021, 8:23:06 PM	8/15/2008, 12:00:00 AM
Vulnerability Description : Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.				
CVE-2010-0742	2.192.0.249	8000	12/25/2021, 8:23:06 PM	6/3/2010, 12:00:00 AM
Vulnerability Description : The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.				
CVE-2012-2311	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.				
CVE-2008-5557	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/23/2008, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.				
CVE-2008-5658	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.				
CVE-2014-8626	2.192.0.249	8000	12/25/2021, 8:23:06 PM	11/23/2014, 12:00:00 AM
Vulnerability Description : Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.				
CVE-2011-3192	2.192.0.249	8000	12/25/2021, 8:23:06 PM	8/29/2011, 12:00:00 AM
Vulnerability Description : The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.				
CVE-2012-2386	2.192.0.249	8000	12/25/2021, 8:23:06 PM	7/7/2012, 12:00:00 AM
Vulnerability Description : Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.				
CVE-2012-2110	2.192.0.249	8000	12/25/2021, 8:23:06 PM	4/19/2012, 12:00:00 AM
Vulnerability Description : The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.				
CVE-2010-4252	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.				
CVE-2009-3245	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/5/2010, 12:00:00 AM
Vulnerability Description : OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.				
CVE-2009-3291	2.192.0.249	8000	12/25/2021, 8:23:06 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : The php_openssl_apply_verification_policy function in PHP before 5.2.11 does not properly perform certificate validation, which has unknown impact and attack vectors, probably related to an ability to spoof certificates.				
CVE-2011-1092	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/15/2011, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.				
CVE-2009-3292	2.192.0.249	8000	12/25/2021, 8:23:06 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in PHP before 5.2.11, and 5.3.x before 5.3.1, has unknown impact and attack vectors related to "missing sanity checks around exif processing."				
CVE-2009-3293	2.192.0.249	8000	12/25/2021, 8:23:06 PM	9/22/2009, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."				
CVE-2014-8176	2.192.0.249	8000	12/25/2021, 8:23:06 PM	6/12/2015, 12:00:00 AM
Vulnerability Description : The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.				
CVE-2017-7679	2.192.0.249	8000	12/25/2021, 8:23:06 PM	6/20/2017, 12:00:00 AM
Vulnerability Description : In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.				
CVE-2010-1868	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/7/2010, 12:00:00 AM
Vulnerability Description : The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.				
CVE-2014-9427	2.192.0.249	8000	12/25/2021, 8:23:06 PM	1/3/2015, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.				
CVE-2008-5624	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.				
CVE-2012-1823	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/11/2012, 12:00:00 AM
Vulnerability Description : sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.				
CVE-2010-2225	2.192.0.249	8000	12/25/2021, 8:23:06 PM	6/24/2010, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.				
CVE-2008-0599	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.				
CVE-2008-7002	2.192.0.249	8000	12/25/2021, 8:23:06 PM	8/19/2009, 12:00:00 AM
Vulnerability Description : PHP 5.2.5 does not enforce (a) open_basedir and (b) safe_mode_exec_dir restrictions for certain functions, which might allow local users to bypass intended access restrictions and call programs outside of the intended directory via the (1) exec, (2) system, (3) shell_exec, (4) passthru, or (5) popen functions, possibly involving pathnames such as "C:" drive notation.				
CVE-2012-2688	2.192.0.249	8000	12/25/2021, 8:23:06 PM	7/20/2012, 12:00:00 AM
Vulnerability Description : Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."				
CVE-2008-2051	2.192.0.249	8000	12/25/2021, 8:23:06 PM	5/5/2008, 12:00:00 AM
Vulnerability Description : The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."				
CVE-2011-3268	2.192.0.249	8000	12/25/2021, 8:23:06 PM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.				
CVE-2010-1129	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/26/2010, 12:00:00 AM
Vulnerability Description : The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.				
CVE-2011-1153	2.192.0.249	8000	12/25/2021, 8:23:06 PM	3/16/2011, 12:00:00 AM
Vulnerability Description : Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.				
CVE-2011-4109	2.192.0.249	8000	12/25/2021, 8:23:06 PM	1/6/2012, 12:00:00 AM
Vulnerability Description : Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.				
CVE-2009-4018	2.192.0.249	8000	12/25/2021, 8:23:06 PM	11/29/2009, 12:00:00 AM
Vulnerability Description : The proc_open function in ext/standard/proc_open.c in PHP before 5.2.11 and 5.3.x before 5.3.1 does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.				
CVE-2008-5625	2.192.0.249	8000	12/25/2021, 8:23:06 PM	12/17/2008, 12:00:00 AM
Vulnerability Description : PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.				
CVE-2016-10009	2.192.2.196	22	12/8/2021, 12:34:48 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-8858	2.192.2.196	22	12/8/2021, 12:34:48 PM	12/9/2016, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10012	2.192.2.196	22	12/8/2021, 12:34:48 PM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2015-5600	2.192.3.183	22	12/8/2021, 12:17:39 PM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2014-1692	2.192.3.183	22	12/8/2021, 12:17:39 PM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2010-4478	2.192.7.56	22	12/8/2021, 8:27:10 AM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				
CVE-2014-1692	2.192.0.81	22	12/8/2021, 5:56:36 AM	1/29/2014, 12:00:00 AM
Vulnerability Description : The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.				
CVE-2015-5600	2.192.0.81	22	12/8/2021, 5:56:36 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2015-5600	2.192.10.30	22	12/8/2021, 5:43:50 AM	8/3/2015, 12:00:00 AM
Vulnerability Description : The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.				
CVE-2016-10012	2.192.6.167	22	12/8/2021, 2:19:41 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-8858	2.192.6.167	22	12/8/2021, 2:19:41 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2016-10009	2.192.6.167	22	12/8/2021, 2:19:41 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-6515	2.192.6.167	22	12/8/2021, 2:19:41 AM	8/7/2016, 12:00:00 AM
Vulnerability Description : The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.				
CVE-2016-10009	2.192.0.173	22	12/8/2021, 12:03:02 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.				
CVE-2016-6515	2.192.0.173	22	12/8/2021, 12:03:02 AM	8/7/2016, 12:00:00 AM
Vulnerability Description : The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.				
CVE-2016-10012	2.192.0.173	22	12/8/2021, 12:03:02 AM	1/4/2017, 12:00:00 AM
Vulnerability Description : The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.				
CVE-2016-8858	2.192.0.173	22	12/8/2021, 12:03:02 AM	12/9/2016, 12:00:00 AM
Vulnerability Description : ** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."				
CVE-2010-4478	2.192.11.10	22	12/7/2021, 10:09:26 PM	12/6/2010, 12:00:00 AM
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				
CVE-2007-4752	2.192.11.10	22	12/7/2021, 10:09:26 PM	9/12/2007, 12:00:00 AM
Vulnerability Description : ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.				
CVE-2010-4478	2.192.4.46	2222	11/16/2021, 1:24:29 AM	12/6/2010, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.				

High-severity CVE patching analyzed

This analysis reflects the number of high-severity CVEs detected in the network, the percentage that were resolved in the past 180 days, and how quickly you apply patches.

Description
We analyze patching coverage for high-severity Common Vulnerabilities and Exposures (CVEs). We base this analysis on the number and percentage of high-severity vulnerabilities that were resolved on the network since their detection, and the average resolution time over a 180-day period. High-severity CVEs have a Common Vulnerability Scoring System (CVSS v2) base score that ranges between 7.0 and 10. While high-severity vulnerabilities warrant more urgent attention, maintaining a regular patching cadence for all vulnerabilities is an important security best practice. See metrics in the table below, including the number of vulnerabilities resolved in different time windows ranging less than 60 days to over 180.

Recommendation
Monitor CVE lists and vulnerability repositories for exploit code that may affect the network infrastructure. Subscribe to the National Vulnerability Database (NVD) RSS or other feeds to learn of new exploits and vulnerabilities as they are released. Maintain a regular updating schedule for all your software and hardware, and apply all the latest patches as they are released. Also, correlate this analysis with individual CVE findings in your Scorecard to help you better understand the effectiveness of your patching practices.

1 finding

ALL ACTIVE IN PAST 180 DAYS	RESOLVED ISSUES	RESOLVED %	AVERAGE DAYS TO RESOLVE	RESOLVED: 60 DAYS OR LESS	RESOLVED: 60-120 DAYS	RESOLVED: 121-180 DAYS	RESOLVED: OVER 180 DAYS	LAST UPDATE
346	203	59	45	200	3			3/13/2022, 12:00:00 AM

Low-Severity Vulnerability in Last Observation

-0.2 SCORE IMPACT

We observed a low-severity vulnerability during our last scan, which may still be publicly exposed.

Description
Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability.
Software and hardware frequently self-report their product name and version when hosts connect to them. By searching through the CVE list and cross-referencing the names and versions of products found on this company's network, we are able to infer the presence of vulnerabilities.

Recommendation
Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits and vulnerabilities as they are released. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they are released.

51 findings

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2018-20685	2.192.2.247	22	1/10/2019, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.2.247	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:35 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2018-20685	2.192.2.167	22	1/10/2019, 12:00:00 AM	3/8/2022, 11:42:27 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.2.167	22	1/4/2017, 12:00:00 AM	3/8/2022, 11:42:27 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2011-5000	2.192.8.188	22	4/5/2012, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.8.188	22	2/3/2014, 12:00:00 AM	3/8/2022, 11:26:06 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2011-5000	2.192.2.9	22	4/5/2012, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.2.9	22	2/3/2014, 12:00:00 AM	3/8/2022, 9:42:01 AM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2018-20685	2.192.8.91	22	1/10/2019, 12:00:00 AM	3/8/2022, 9:28:05 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2018-20685	2.192.10.198	22	1/10/2019, 12:00:00 AM	3/8/2022, 8:36:38 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2018-20685	2.192.5.233	22	1/10/2019, 12:00:00 AM	3/8/2022, 7:43:57 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.2.120	22	8/24/2015, 12:00:00 AM	3/8/2022, 6:04:00 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2015-6563	2.192.2.119	22	8/24/2015, 12:00:00 AM	3/8/2022, 6:02:46 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.4.204	22	1/10/2019, 12:00:00 AM	3/8/2022, 5:34:05 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.4.31	22	8/24/2015, 12:00:00 AM	3/8/2022, 5:28:55 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2015-6563	2.192.5.95	22	8/24/2015, 12:00:00 AM	3/8/2022, 12:55:13 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.4.164	22	1/10/2019, 12:00:00 AM	3/7/2022, 11:25:39 PM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2015-6563	2.192.9.114	22	8/24/2015, 12:00:00 AM	3/7/2022, 11:12:49 PM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2014-5459	2.192.0.124	8080	9/27/2014, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.				
CVE-2006-4625	2.192.0.124	8080	9/12/2006, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : PHP 4.x up to 4.4.4 and PHP 5 up to 5.1.6 allows local users to bypass certain Apache HTTP Server httpd.conf options, such as safe_mode and open_basedir, via the ini_restore function, which resets the values to their php.ini (Master Value) defaults.				
CVE-2008-5814	2.192.0.124	8080	1/2/2009, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.				
CVE-2008-0456	2.192.0.124	8080	1/25/2008, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : CRLF injection vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.				
CVE-2007-2509	2.192.0.124	8080	5/9/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM
Vulnerability Description : CRLF injection vulnerability in the ftp_putcmd function in PHP before 4.4.7, and 5.x before 5.2.2 allows remote attackers to inject arbitrary FTP commands via CRLF sequences in the parameters to earlier FTP commands.				
CVE-2007-2727	2.192.0.124	8080	5/16/2007, 12:00:00 AM	2/27/2022, 8:38:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The mcrypt_create_iv function in ext/mcrypt/mcrypt.c in PHP before 4.4.7, 5.2.1, and possibly 5.0.x and other PHP 5 versions, calls php_rand_r with an uninitialized seed variable and therefore always generates the same initialization vector (IV), which might allow context-dependent attackers to decrypt certain data more easily because of the guessable encryption keys.				
CVE-2012-2687	2.192.5.76	80	8/22/2012, 12:00:00 AM	2/12/2022, 4:34:44 AM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2012-2687	2.192.3.142	80	8/22/2012, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2016-7056	2.192.3.142	80	9/10/2018, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.				
CVE-2013-0169	2.192.3.142	80	2/8/2013, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.				
CVE-2011-1945	2.192.3.142	80	5/31/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.				
CVE-2014-5459	2.192.3.142	80	9/27/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.				
CVE-2008-5814	2.192.3.142	80	1/2/2009, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : Cross-site scripting (XSS) vulnerability in PHP, possibly 5.2.7 and earlier, when display_errors is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: because of the lack of details, it is unclear whether this is related to CVE-2006-0208.				
CVE-2014-0076	2.192.3.142	80	3/25/2014, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.				
CVE-2011-4415	2.192.3.142	80	11/8/2011, 12:00:00 AM	2/11/2022, 8:52:12 PM
Vulnerability Description : The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.				
CVE-2019-1547	2.192.3.2	80	9/10/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2018-5407	2.192.3.2	80	11/15/2018, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.				
CVE-2019-1552	2.192.3.2	80	7/30/2019, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).				
CVE-2020-7068	2.192.3.2	80	9/9/2020, 12:00:00 AM	2/11/2022, 2:44:31 AM
Vulnerability Description : In PHP versions 7.2.x below 7.2.33, 7.3.x below 7.3.21 and 7.4.x below 7.4.9, while processing PHAR files using phar extension, phar_parse_zipfile could be tricked into accessing freed memory, which could lead to a crash or information disclosure.				
CVE-2014-0076	2.192.9.190	80	3/25/2014, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.				
CVE-2013-0169	2.192.9.190	80	2/8/2013, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.				
CVE-2011-4415	2.192.9.190	80	11/8/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.				
CVE-2016-7056	2.192.9.190	80	9/10/2018, 12:00:00 AM	2/10/2022, 11:59:49 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.				
CVE-2011-1945	2.192.9.190	80	5/31/2011, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.				
CVE-2012-2687	2.192.9.190	80	8/22/2012, 12:00:00 AM	2/10/2022, 11:59:49 AM
Vulnerability Description : Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2016-10011	2.192.4.184	22	1/4/2017, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2018-20685	2.192.4.184	22	1/10/2019, 12:00:00 AM	2/8/2022, 3:36:45 PM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2011-5000	2.192.4.252	22	4/5/2012, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.				
CVE-2011-4327	2.192.4.252	22	2/3/2014, 12:00:00 AM	2/8/2022, 3:35:18 PM
Vulnerability Description : ssh-keysign.c in ssh-keysign in OpenSSH before 5.8p2 on certain platforms executes ssh-rand-helper with unintended open file descriptors, which allows local users to obtain sensitive key information via the ptrace system call.				
CVE-2018-20685	2.192.4.221	22	1/10/2019, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				
CVE-2016-10011	2.192.4.221	22	1/4/2017, 12:00:00 AM	2/8/2022, 10:15:59 AM
Vulnerability Description : authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.				
CVE-2015-6563	2.192.11.227	22	8/24/2015, 12:00:00 AM	2/8/2022, 7:40:14 AM
Vulnerability Description : The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.				
CVE-2018-20685	2.192.8.230	22	1/10/2019, 12:00:00 AM	2/7/2022, 11:56:47 PM
Vulnerability Description : In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.				

A 100 SOCIAL ENGINEERING

The SecurityScorecard Social Engineering Module is used to determine the potential susceptibility of an organization to a targeted social engineering attack. The Social Engineering module ingests data from social networks and public data breaches, and blends proprietary analysis methods. The Social Engineering Score is an informational indicator calculated based on the quantity of indicators that appear in SecurityScorecard collection sensors.

HIGH SEVERITY
There are no High Severity Issues for Social Engineering

MEDIUM SEVERITY
There are no Medium Severity Issues for Social Engineering

LOW SEVERITY
There are no Low Severity Issues for Social Engineering

POSITIVE
There are no Positive Signals for Social Engineering

INFORMATIONAL

Exposed Personal Information (Historical)	1

Exposed Personal Information (Historical)

Personal information for individuals associated with employee emails were exposed.

Description
Social engineering attacks are significantly more effective when they are used in combination with exposed personal information. For example, security questions to reset account passwords, or to recover accounts that require personal information. Additionally, it's easier for hackers to impersonate employees to gain higher level access. Please note that SecurityScorecard only sees the categories of information associated with exposure.
For privacy reasons, affected user names are only visible to the Administrator of the respective account and are not displayed for other scorecards than you follow.

Recommendation
It's not feasible to remove the information off the internet once exposed so mitigation against social engineering attacks are recommended. Ensure that:
* employees have regular cyber security awareness training * protocols are established for handling sensitive information * periodic, unannounced, tests are performed.

1 finding

DOMAIN	LEAK NAME	LEAK YEAR	DESCRIPTION	AFFECTED USERS	LAST OBSERVED
ovofinance.com	RankWatch.com	2016	RankWatch is an SEO marketing platform that gives a way for companies to see all the aspects of digital and Internet marketing used. The leak is from a exposed mongoDB and looks like most of the information was gathered, probably by scrappers and other 3party apps. More then 40Million emails and other information got leaked.	contact	8/31/2019, 12:00:00 AM

No content (including ratings, data, reports, software or other application or output therefrom) or any part thereof (collectively, Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system without the prior written permission of SecurityScorecard, Inc. (SSC) The Content shall not be used for any unlawful or unauthorized purposes.

SSC and any third-parties, and their directors, officers, shareholders, employees, customers and agents (collectively SSC Parties) do not guarantee or warrant the accuracy, completeness, timeliness or availability of the Content. SSC Parties are not responsible for any errors or omissions (negligent or otherwise), regardless of the cause, or for the results obtained from the use of the Content. The Content is provided on an "as is" basis. SSC PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS,(3) FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall SSC Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

USERS OF THE CONTENT MUST USE ALL REASONABLE ENDEAVORS TO MITIGATE ANY LOSS OR DAMAGE WHATSOEVER (AND HOWSOEVER ARISING) AND NOTHING HEREIN SHALL BE DEEMED TO RELIEVE OR ABROGATE USERS OF ANY SUCH DUTY TO MITIGATE ANY LOSS OR DAMAGE.

IN ANY EVENT, TO THE EXTENT PERMITTED BY LAW, THE AGGREGATE LIABILITY OF THE SSC PARTIES FOR ANY REASON WHATSOEVER RELATED TO ACCESS TO OR USE OF CONTENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL AMOUNT PAID TO SSC BY THE USER FOR SERVICES PROVIDED DURING THE 12 MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO LIABILITY, AND (B) U.S. $100.

Security-related analyses, including ratings and statements in the Content, are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations regarding decision to do business with any entity, endorsements of the accuracy of any of the data or conclusions or attempts to independently assess or vouch for the security measures of any entity. SSC’s opinions, analyses and ratings should not be relied on as a substitute for the skill, judgment and experience of the user and its management, employees, advisors and clients when making business decisions. SSC assumes no obligation to update the Content following publication in any form or format. While SSC has obtained information from sources it believes to be reliable, SSC does not perform an audit and undertakes no duty of due diligence or independent verification of any information it receives. Users expressly agree that (a) the security ratings and other security opinions provided via the Content do not reflect, identify or detect every vulnerability or security issue or address any other risk; (b) the security ratings and other opinions provided do not take into account users’ particular objectives, situations or needs; (c) each rating or other opinion will be weighed, if at all, solely as one factor in any decision made by or on behalf of any user; and (d) users will accordingly, with due care, make their own study and evaluation of the risks of doing business with any entity. If a user identifies any in the Content, we invite you to share that information with us by emailing us at support@securityscorecard.io.