



## DETAILED REPORT

# Scorecard for New York University

Generated **March 15, 2020**

by Mike Wilkes (mwilkes@ascap.com), ASCAP

## About this report

This report is a point-in-time capture of this Scorecard as of 3:22:29 AM UTC, March 15, 2020. 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](https://bit.ly/2P8okyb).

Learn more about SecurityScorecard at [bit.ly/2xXNg4N](https://bit.ly/2xXNg4N) today.

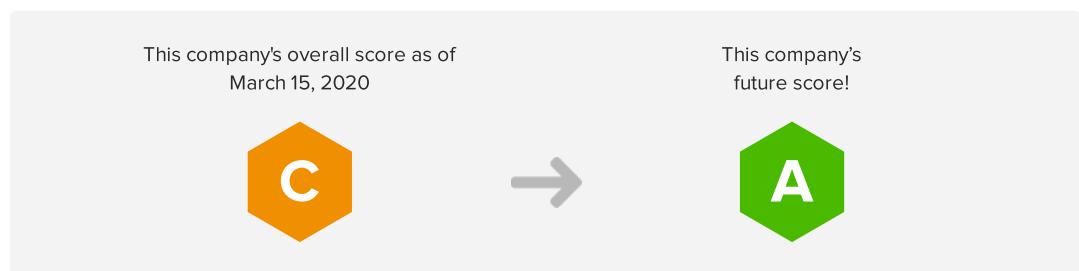
## What is SecurityScorecard?

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<sup>1</sup>. 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](https://bit.ly/2zMLSmW).

<sup>1</sup> "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 organization'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](mailto: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](mailto:support@securityscorecard.io).

# Scorecard Overview



**New York University**

74 Security Score

DOMAIN: nyu.edu

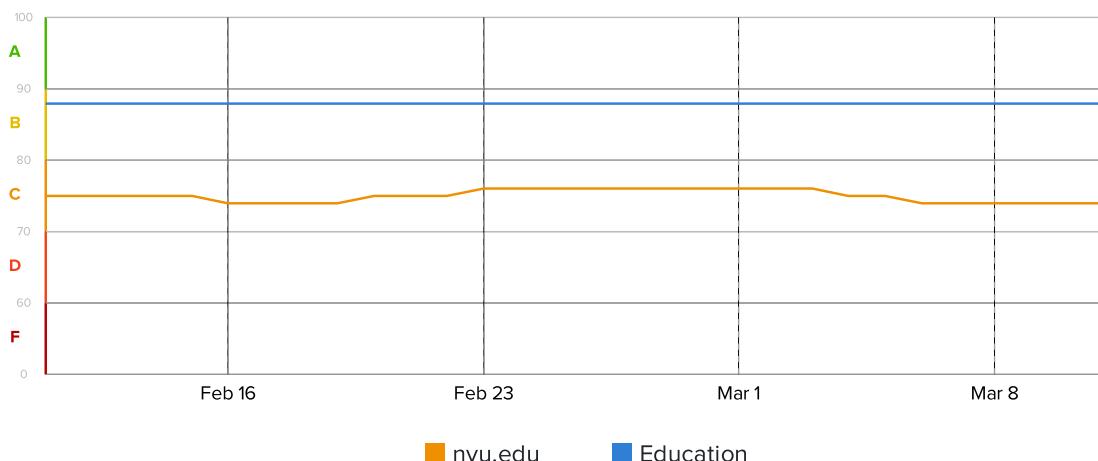
INDUSTRY: EDUCATION

## Factors

<span style="color: green;">A</span> 100 CUBIT SCORE	1 ISSUE	<span style="color: orange;">C</span> 72 ENDPOINT SECURITY	2 ISSUES
<span style="color: green;">A</span> 100 INFORMATION LEAK	0 ISSUES	<span style="color: orange;">C</span> 77 IP REPUTATION	3 ISSUES
<span style="color: red;">D</span> 65 NETWORK SECURITY	21 ISSUES	<span style="color: red;">D</span> 69 DNS HEALTH	2 ISSUES
<span style="color: green;">A</span> 100 HACKER CHATTER	0 ISSUES	<span style="color: green;">A</span> 100 SOCIAL ENGINEERING	0 ISSUES
<span style="color: orange;">C</span> 70 PATCHING CADENCE	8 ISSUES	<span style="color: orange;">C</span> 72 APPLICATION SECURITY	14 ISSUES

## 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 issues, 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
Network Security	!!!	-0.6	Certificate Is Revoked. Revoked certificates prevent TLS clients from connecting to servers.
	!!!	-0.6	SSH Software Supports Vulnerable Protocol. Server(s) observed running SSH software that support an SSH protocol lower than version 2.
	!!!	-0.5	MongoDB Service Observed. We observed MongoDB, a database management system, publicly exposed.
	!!	-0.6	VNC Service Observed. We observed VNC, a remote access service, publicly exposed.
	!!	-0.1	SMB Service Observed. We observed SMB, a file and printer-sharing service, publicly exposed.
	!!	-0.4	MySQL Service Observed. We observed MySQL, a database management system, publicly exposed.
	!!	-0.3	SSH Supports Weak MAC. A weak Message Authentication Code (MAC) algorithm has been detected.
	!!	-0.2	RDP Service Observed. We observed RDP, a remote access service, publicly exposed.
	!!	-0.7	TLS Protocol Uses Weak Cipher. TLS analysis reveals a weak cipher either through encryption protocol or public key length.
	!!	-0.3	rsync Service Observed. We observed rsync, a file-sharing service, publicly exposed.
	!!	-0.6	Certificate Is Expired. Expired certificates prevent TLS clients from connecting to servers.
	!!	-0.3	SSH Supports Weak Cipher. A weak cipher has been detected.
	!!	-0.3	IMAP Service Observed. We observed IMAP, an email retrieval service, publicly exposed.
	!!	-0.3	Certificate Is Self-Signed. Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.
	!	-0.1	FTP Service Observed. We observed FTP, a file-sharing service, publicly exposed.
	!	-<0.1	Telnet Service Observed. We observed Telnet, a remote access service, publicly exposed.
	!	-0.2	TLS Certificate Without Revocation Control. We observed a TLS certificate that did not contain either CRL or OCSP URLs.
	!	-0.2	Certificate Lifetime Is Longer Than Best Practices. We observed a certificate with a lifetime longer than 39 Months.
Patching Cadence	!!!	-1.1	High-Severity Vulnerability in Last Observation. We observed a high-severity vulnerability during our last scan, which may still be publicly exposed.
	!!!	-1.2	High Severity CVEs Patching Cadence. High severity vulnerability seen on network more than 30 days after CVE was published.

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
Network Infrastructure	!!	-0.1	End-of-Service Product. We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.
	!!	-0.7	Medium Severity CVEs Patching Cadence. Medium severity vulnerability seen on network more than 60 days after CVE was published.
	!!	<-0.1	End-of-Life Product. We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.
	!!	-0.8	Medium-Severity Vulnerability in Last Observation. We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.
	!	-0.3	Low-Severity Vulnerability in Last Observation. We observed a low-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 180 days after CVE was published.
	!	-2.1	Outdated Web Browser Observed. An outdated web browser connected to a web server.
Endpoint Security	!!	-1.0	Outdated Operating System Observed. A web browser on an outdated operating system connected to a web server.
	!!!	-	Malware Events, Last Day. Communications indicative of malware infections were observed over the last 24 hours.
	!!	-2.7	Malware Events, Last Month. Communications indicative of malware infections were observed over the last 30 days.
IP Reputation	!	-	Malware Events, Last Year. Communications indicative of malware infections were observed over the last 365 days.
	!	-1.7	SPF Record Missing. A missing SPF record has been detected for a domain.
DNS Health	!	-0.5	SPF Record Contains a Softfail. Softfail attributes in SPF makes spoofing and phishing email possible.
	!!!	-0.4	Site does not enforce HTTPS. Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).
Application Security	!!	-0.3	Website does not implement X-Frame-Options Best Practices. Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.
	!!	-0.3	Website does not implement X-XSS-Protection Best Practices. Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.
	!!	-0.5	Redirect Chain Contains HTTP. Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.
	!!	-0.5	Website Does Not Implement HSTS Best Practices. Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.

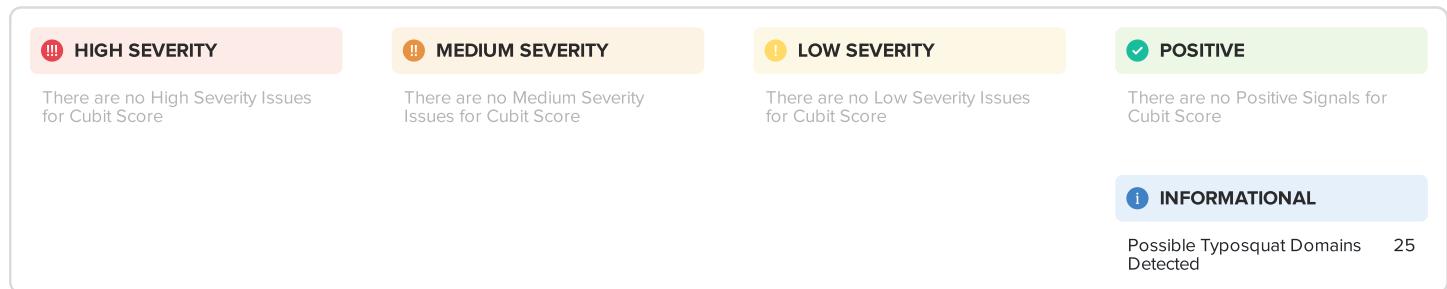
Security-related analyses, including ratings, and statements in the Content of this document are statements of opinion of relative future security risks of entities as of the date they are expressed, and not statements of current or historical fact as to safety of transacting with any entity, recommendations 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

FACTOR	SEVERITY	SCORE IMPACT	ISSUES DETECTED
		-0.5	Insecure HTTPS Redirect Pattern. Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.
		-0.1	Website does not implement X-Content-Type-Options Best Practices. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

# 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



## i Possible Typosquat Domains Detected

Domains have been detected which may be an indication of typosquat.

### Description

This is an informational issue and is not calculated as part of the score. Typosquatting, also called URL hijacking, a sting site, or a fake URL, is a form of cybersquatting in which malicious actors register domains that are similar to legitimate domains but contain a common misspelling or a different TLD (Top-Level Domain). This attack relies on the possibility that a user will accidentally mis-type a URL and arrive at the attacker-controlled site instead of their intended destination. In a related practice, called Homograph Attacks, attackers register domains that look visually similar to existing domains (replacing an 'I' with an 'I' or a '1' for example) using similar ASCII characters or in some cases unicode characters that are visually indistinguishable from their equivalent ASCII characters. These attacks can also be used as part of a phishing campaign to deceive email recipients into clicking on a link that leads to an attacker-controlled website. As a best practice, some organizations who utilize brand reputation and domain protection services, may intentionally register similar domains to deter malicious actors from creating typosquatted domains.

### Recommendation

Verify that the typosquat domain does not pose a risk to the organization. If necessary, perform a domain take-down of malicious domains which may be used for phishing.

### 25 findings

IP ADDRESS	DOMAIN	LAST OBSERVED
198.54.117.217	www.nyu.exposed	2/20/2020, 9:41:58 PM
68.65.122.10	mail.nyu.singles	2/20/2020, 9:41:57 PM
89.40.32.94	www.nyu.best	2/20/2020, 9:41:57 PM
68.178.252.117	imap.nyu.asia	2/20/2020, 9:41:57 PM

IP ADDRESS	DOMAIN	LAST OBSERVED
173.201.192.129	mail.nyu.asia	2/20/2020, 9:41:57 PM
217.70.178.4	pop.nyu.pw	2/20/2020, 9:41:57 PM
217.26.49.199	pop.nyu.li	2/20/2020, 9:41:57 PM
13.124.227.113	xp.nyu.in	2/20/2020, 9:41:57 PM
199.253.30.165	www.nyu.xxx	2/20/2020, 9:41:57 PM
188.93.95.11	xp.nyu.80	2/20/2020, 9:41:57 PM
64.70.19.203	xp.nyu.ws	2/20/2020, 9:41:57 PM
88.198.29.97	xp.nyu.vg	2/20/2020, 9:41:57 PM
185.53.178.8	xp.nyu.uk	2/20/2020, 9:41:57 PM
188.128.255.251	xp.nyu.pl	2/20/2020, 9:41:57 PM
45.79.222.138	xp.nyu.ph	2/20/2020, 9:41:57 PM
213.136.12.232	xp.nyu.nl	2/20/2020, 9:41:57 PM
173.230.141.80	xp.nyu.la	2/20/2020, 9:41:57 PM
195.70.38.180	xp.nyu.hu	2/20/2020, 9:41:57 PM
198.74.54.240	xp.nyu.fm	2/20/2020, 9:41:57 PM
83.136.252.35	xp.nyu.fi	2/20/2020, 9:41:57 PM
185.53.179.6	xp.nyu.es	2/20/2020, 9:41:57 PM
47.91.169.15	xp.nyu.cn	2/20/2020, 9:41:57 PM
217.26.51.214	xp.nyu.li	2/20/2020, 9:41:57 PM
69.172.201.153	xp.nyu.com	2/20/2020, 9:41:57 PM
199.59.242.153	xp.nyu.tv	2/20/2020, 9:41:57 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

### i INFORMATIONAL

There are no Informational Signals for Information Leak

No issues found



## 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		!! MEDIUM SEVERITY		! LOW SEVERITY		✓ POSITIVE	
Certificate Is Revoked	2	VNC Service Observed	190	FTP Service Observed	58	TLS Certificate Status Request ("OCSP Stapling") Detected	51
SSH Software Supports Vulnerable Protocol	11	SMB Service Observed	2	Telnet Service Observed	16	Extended Validation Certificate Observed	2
MongoDB Service Observed	2	MySQL Service Observed	33	TLS Certificate Without Revocation Control	55		
		SSH Supports Weak MAC	109	Certificate Lifetime Is Longer Than Best Practices	12		
		RDP Service Observed	10				
		TLS Protocol Uses Weak Cipher	82				
		rsync Service Observed	5				
		Certificate Is Expired	53				
		SSH Supports Weak Cipher	502				
		IMAP Service Observed	27				
		Certificate Is Self-Signed	4				
ℹ INFORMATIONAL							
						POP3 Service Observed	28

# ! FTP Service Observed

-0.1 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 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.

## 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 whitelisting the IP addresses that require access.

58 findings

Product Name	Product Version	IP Address	Port	Last Observed
ProFTPD	1.3.1	159.65.160.172	119	3/11/2020, 1:40:25 PM
ProFTPD	1.3.1	159.65.160.172	445	3/10/2020, 10:29:03 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
ProFTPD	1.3.1	159.65.160.172	5901	3/8/2020, 8:52:32 PM
ProFTPD	1.3.4c	128.122.33.16	21	3/4/2020, 2:52:14 AM
Pure-FTPd		37.60.232.214	21	3/4/2020, 2:22:44 AM
		192.76.177.246	21	3/4/2020, 2:16:50 AM
FileZilla ftpd		128.122.136.13	21	3/4/2020, 1:56:12 AM
vsftpd	2.3.2	128.122.136.84	21	3/4/2020, 1:54:33 AM
oftpd		128.122.201.233	21	3/4/2020, 12:45:16 AM
Microsoft ftpd		128.122.49.92	21	3/4/2020, 12:09:24 AM
Pure-FTPd		107.180.61.237	21	3/3/2020, 11:36:44 PM
ProFTPD		70.32.92.51	21	3/3/2020, 11:15:24 PM
vsftpd	3.0.3	128.122.4.40	21	3/3/2020, 10:54:00 PM
FileZilla ftpd	0.9.45 beta	128.122.183.228	21	3/3/2020, 10:37:20 PM
vsftpd	2.0.8 or later	128.238.147.209	21	3/3/2020, 10:10:05 PM
vsftpd	2.3.2	128.122.136.82	21	3/3/2020, 9:36:38 PM
FileZilla ftpd		128.122.201.108	21	3/3/2020, 9:29:04 PM
Microsoft ftpd		128.122.141.64	21	3/3/2020, 9:09:16 PM
vsftpd	2.0.4+ (ext.3)	128.122.141.94	21	3/3/2020, 9:08:24 PM
CrushFTP		128.122.141.174	21	3/3/2020, 9:04:08 PM
vsftpd	2.3.2	128.122.136.83	21	3/3/2020, 8:56:14 PM
tnftpd	20100324+GSSAPI	216.165.116.103	21	3/3/2020, 8:12:21 PM
vsftpd	2.0.8 or later	91.230.41.23	21	3/3/2020, 7:51:42 PM
vsftpd		216.165.21.221	21	3/3/2020, 7:39:27 PM
FileZilla ftpd		128.122.80.48	21	3/3/2020, 7:34:27 PM
Axis P1425-E Network Camera ftpd	6.50.3	128.122.164.28	21	3/3/2020, 7:29:29 PM
Axis P3364 Fixed Dome Network Camera ftpd	6.10.1.3	128.122.35.10	21	3/3/2020, 7:29:04 PM
ProFTPD		70.32.96.242	21	3/3/2020, 7:01:47 PM
Pure-FTPd		128.238.31.104	21	3/3/2020, 6:59:41 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Pure-FTPd		128.122.131.35	21	3/3/2020, 6:55:34 PM
vsftpd	3.0.3	128.122.60.249	21	3/3/2020, 6:17:45 PM
Computer Solutions RT-IP ftpd		192.76.177.142	21	3/3/2020, 6:16:49 PM
Axis P3225-LVE Network Camera ftpd	6.50.3	128.122.164.37	21	3/3/2020, 5:24:44 PM
Aruba router ftpd		192.76.177.149	21	3/3/2020, 5:22:28 PM
FileZilla ftpd		128.122.184.51	21	3/3/2020, 4:55:14 PM
NET Disk/NetStore ftpd		128.122.93.207	21	3/3/2020, 4:21:33 PM
Microsoft ftpd		216.165.117.135	21	3/3/2020, 3:54:37 PM
ProFTPD	1.3.4a	128.122.133.17	21	3/3/2020, 3:50:16 PM
Pure-FTPd		35.214.191.115	21	3/3/2020, 3:16:40 PM
ProFTPD	1.3.4a	128.122.133.16	21	3/3/2020, 3:11:20 PM
tnftpd	20080929	128.122.28.100	21	3/3/2020, 2:43:52 PM
ProFTPD or KnFTPD		128.238.26.21	21	3/3/2020, 2:05:47 PM
Pure-FTPd		128.122.30.9	21	3/3/2020, 1:52:24 PM
TRENDnet/Hawking webcam ftpd		128.122.71.177	21	3/3/2020, 1:46:16 PM
		128.122.161.203	21	3/3/2020, 1:39:30 PM
Mac OS X Server ftpd		128.122.161.197	21	3/3/2020, 1:39:19 PM
ProFTPD	1.3.1	159.65.160.172	6000	3/2/2020, 1:12:50 PM
ProFTPD	1.3.1	159.65.160.172	4040	2/22/2020, 9:08:39 PM
ProFTPD	1.3.1	159.65.160.172	666	2/16/2020, 2:17:45 PM
vsftpd	2.0.1	195.113.82.217	21	2/14/2020, 6:37:13 AM
		159.65.160.172	21	2/14/2020, 5:12:12 AM
Computer Solutions RT-IP ftpd		192.76.177.141	21	2/14/2020, 4:35:15 AM
FileZilla ftpd		128.122.141.22	990	2/14/2020, 12:39:15 AM
oftpd		128.122.201.233	990	2/13/2020, 11:18:34 PM
vsftpd	2.3.2	128.122.136.85	21	2/4/2020, 7:30:38 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
Brother/HP printer ftpd	1.13	128.122.63.8	21	2/4/2020, 6:46:04 PM
GNU Inetutils FTPd	1.3.2	128.122.228.195	21	2/4/2020, 4:22:01 PM
Computer Solutions RT-IP ftpd		192.76.177.140	21	2/4/2020, 3:26:19 PM

## !! VNC Service Observed

-0.6 SCORE IMPACT

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

### Description

The VNC 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 a VNC 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. 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.

### 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 whitelisting the IP addresses that require access.

190 findings

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
Apple remote desktop vnc		195.113.94.166	5900	3/11/2020, 12:55:21 AM
Apple remote desktop vnc		195.113.94.79	5900	3/10/2020, 8:09:53 PM
Apple remote desktop vnc		128.238.149.12	5900	3/10/2020, 2:39:58 PM
Apple remote desktop vnc		193.175.54.117	5900	3/10/2020, 4:50:08 AM
Apple remote desktop vnc		193.175.54.120	5900	3/10/2020, 1:53:22 AM
Apple remote desktop vnc		195.113.94.141	5900	3/9/2020, 6:01:44 PM
Apple remote desktop vnc		193.175.54.123	5900	3/9/2020, 1:54:00 PM
Apple remote desktop vnc		195.113.94.167	5900	3/9/2020, 4:22:14 AM
VNC		192.86.139.76	5900	2/28/2020, 2:21:50 PM
Apple remote desktop vnc		193.175.54.107	5900	2/28/2020, 2:19:20 PM

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		193.175.54.93	5900	2/28/2020, 2:19:01 PM
VNC		192.86.139.73	5900	2/28/2020, 2:15:39 PM
Apple remote desktop vnc		128.238.7.138	5900	2/28/2020, 2:14:18 PM
VNC		192.86.139.74	5900	2/28/2020, 2:10:44 PM
Apple remote desktop vnc		193.175.54.95	5900	2/28/2020, 1:59:27 PM
Apple remote desktop vnc		193.175.54.81	5900	2/28/2020, 1:55:39 PM
VNC		192.86.139.71	5900	2/28/2020, 1:55:22 PM
VNC		192.86.139.68	5900	2/28/2020, 1:51:01 PM
Apple remote desktop vnc		195.113.94.168	5900	2/23/2020, 4:59:51 PM
VNC		128.122.185.151	5900	2/19/2020, 9:17:24 AM
Apple remote desktop vnc		128.122.70.171	5900	2/19/2020, 9:10:33 AM
Apple remote desktop vnc		128.122.251.199	5900	2/19/2020, 9:04:56 AM
Apple remote desktop vnc		128.122.81.210	5900	2/19/2020, 9:04:00 AM
Apple remote desktop vnc		128.122.251.16	5900	2/19/2020, 9:03:06 AM
RealVNC Enterprise	5.3 or later	128.122.148.6	5900	2/19/2020, 9:01:02 AM
Apple remote desktop vnc		128.122.102.203	5900	2/19/2020, 8:55:02 AM
Apple remote desktop vnc		128.122.66.135	5900	2/19/2020, 8:51:33 AM
Apple remote desktop vnc		128.122.89.207	5900	2/19/2020, 8:49:26 AM
Apple remote desktop vnc		128.122.68.252	5900	2/19/2020, 8:48:56 AM
Apple remote desktop vnc		128.122.68.242	5900	2/19/2020, 8:48:02 AM
Apple remote desktop vnc		128.122.68.245	5900	2/19/2020, 8:47:05 AM
Apple remote desktop vnc		128.122.115.133	5900	2/19/2020, 8:42:54 AM
Apple remote desktop vnc		128.122.115.147	5900	2/19/2020, 8:41:19 AM
Apple remote desktop vnc		128.122.115.149	5900	2/19/2020, 8:41:05 AM
Apple remote desktop vnc		128.122.115.81	5900	2/19/2020, 8:40:38 AM
Apple remote desktop vnc		128.122.45.65	5900	2/19/2020, 8:38:33 AM
Apple remote desktop vnc		128.122.149.235	5900	2/19/2020, 8:38:19 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		128.122.45.144	5900	2/19/2020, 8:37:07 AM
Apple remote desktop vnc		128.122.45.40	5900	2/19/2020, 8:36:21 AM
Apple remote desktop vnc		128.122.45.234	5900	2/19/2020, 8:36:20 AM
Apple remote desktop vnc		128.122.45.158	5900	2/19/2020, 8:36:10 AM
Apple remote desktop vnc		128.122.45.66	5900	2/19/2020, 8:35:28 AM
Apple remote desktop vnc		128.122.45.64	5900	2/19/2020, 8:35:20 AM
Apple remote desktop vnc		128.122.73.139	5900	2/19/2020, 8:33:22 AM
Apple remote desktop vnc		128.122.94.58	5900	2/19/2020, 8:31:28 AM
Apple remote desktop vnc		128.122.35.6	5900	2/19/2020, 8:24:36 AM
Apple remote desktop vnc		128.122.35.7	5900	2/19/2020, 8:24:14 AM
Apple remote desktop vnc		128.122.35.101	5900	2/19/2020, 8:24:05 AM
Apple remote desktop vnc		128.122.186.82	5900	2/19/2020, 8:24:00 AM
Apple remote desktop vnc		128.122.161.205	5900	2/19/2020, 8:17:03 AM
Apple remote desktop vnc		128.122.161.136	5900	2/19/2020, 8:16:57 AM
Apple remote desktop vnc		128.122.161.178	5900	2/19/2020, 8:16:49 AM
Apple remote desktop vnc		128.122.161.110	5900	2/19/2020, 8:16:47 AM
Apple remote desktop vnc		128.122.161.200	5900	2/19/2020, 8:16:21 AM
RealVNC Personal		128.122.223.204	5900	2/19/2020, 8:14:24 AM
Apple remote desktop vnc		128.122.111.34	5900	2/19/2020, 8:13:59 AM
VNC		128.122.161.15	5900	2/19/2020, 8:05:27 AM
Apple remote desktop vnc		128.122.31.94	5900	2/19/2020, 8:05:15 AM
Apple remote desktop vnc		128.122.31.65	5900	2/19/2020, 8:04:57 AM
Apple remote desktop vnc		128.122.10.140	5900	2/19/2020, 8:03:15 AM
Apple remote desktop vnc		128.122.31.61	5900	2/19/2020, 8:02:33 AM
Apple remote desktop vnc		128.122.250.45	5900	2/19/2020, 8:02:18 AM
Apple remote desktop vnc		128.122.250.34	5900	2/19/2020, 8:02:17 AM
Apple remote desktop vnc		128.122.88.111	5900	2/19/2020, 8:01:28 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		128.122.30.9	5900	2/19/2020, 8:01:09 AM
Apple remote desktop vnc		128.122.88.115	5900	2/19/2020, 8:01:03 AM
Apple remote desktop vnc		128.122.88.47	5900	2/19/2020, 8:01:02 AM
Apple remote desktop vnc		128.122.35.79	5900	2/19/2020, 8:01:00 AM
Apple remote desktop vnc		128.122.30.10	5900	2/19/2020, 8:00:36 AM
Apple remote desktop vnc		128.122.88.142	5900	2/19/2020, 8:00:35 AM
Apple remote desktop vnc		128.122.110.180	5900	2/19/2020, 8:00:32 AM
Apple remote desktop vnc		128.122.35.200	5900	2/19/2020, 8:00:17 AM
Apple remote desktop vnc		128.122.110.116	5900	2/19/2020, 8:00:06 AM
Apple remote desktop vnc		128.122.35.170	5900	2/19/2020, 8:00:04 AM
Apple remote desktop vnc		128.122.35.189	5900	2/19/2020, 7:59:44 AM
Apple remote desktop vnc		128.122.110.108	5900	2/19/2020, 7:59:44 AM
Apple remote desktop vnc		128.122.35.102	5900	2/19/2020, 7:59:38 AM
Apple remote desktop vnc		128.122.110.161	5900	2/19/2020, 7:58:51 AM
VNC		216.165.113.245	5900	2/19/2020, 7:55:11 AM
Apple remote desktop vnc		128.122.115.124	5900	2/19/2020, 7:52:35 AM
Apple remote desktop vnc		128.122.90.112	5900	2/19/2020, 7:48:30 AM
Apple remote desktop vnc		128.122.90.49	5900	2/19/2020, 7:47:58 AM
Apple remote desktop vnc		128.122.89.245	5900	2/19/2020, 7:47:00 AM
VNC		216.165.112.204	5900	2/19/2020, 7:46:26 AM
Apple remote desktop vnc		128.122.92.149	5900	2/19/2020, 7:45:20 AM
Apple remote desktop vnc		128.122.11.122	5900	2/19/2020, 7:42:12 AM
Apple remote desktop vnc		128.122.11.140	5900	2/19/2020, 7:41:48 AM
Apple remote desktop vnc		128.122.28.96	5900	2/19/2020, 7:39:14 AM
Apple remote desktop vnc		128.122.45.28	5900	2/19/2020, 7:34:20 AM
Apple remote desktop vnc		128.122.45.172	5900	2/19/2020, 7:34:11 AM
Apple remote desktop vnc		128.122.73.237	5900	2/19/2020, 7:33:59 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		216.165.113.145	5900	2/19/2020, 7:33:40 AM
VNC		216.165.113.239	5900	2/19/2020, 7:32:42 AM
Apple remote desktop vnc		128.122.100.14	5900	2/19/2020, 7:27:16 AM
Apple remote desktop vnc		128.122.90.37	5900	2/19/2020, 7:27:13 AM
Apple remote desktop vnc		128.122.90.152	5900	2/19/2020, 7:26:47 AM
Apple remote desktop vnc		128.122.89.244	5900	2/19/2020, 7:26:16 AM
Apple remote desktop vnc		128.122.90.40	5900	2/19/2020, 7:26:11 AM
Apple remote desktop vnc		128.122.90.59	5900	2/19/2020, 7:26:07 AM
Apple remote desktop vnc		128.122.100.23	5900	2/19/2020, 7:25:53 AM
Apple remote desktop vnc		128.122.90.41	5900	2/19/2020, 7:25:49 AM
Apple remote desktop vnc		128.122.90.84	5900	2/19/2020, 7:25:35 AM
Apple remote desktop vnc		128.122.90.53	5900	2/19/2020, 7:25:18 AM
Apple remote desktop vnc		128.122.90.60	5900	2/19/2020, 7:24:51 AM
Apple remote desktop vnc		128.122.115.251	5900	2/19/2020, 7:21:00 AM
Apple remote desktop vnc		128.122.86.16	5900	2/19/2020, 7:20:26 AM
Apple remote desktop vnc		128.122.61.8	5900	2/19/2020, 7:19:22 AM
Apple remote desktop vnc		128.122.61.22	5900	2/19/2020, 7:18:06 AM
Apple remote desktop vnc		128.122.110.68	5900	2/19/2020, 7:17:12 AM
Apple remote desktop vnc		128.122.111.4	5900	2/19/2020, 7:15:20 AM
Apple remote desktop vnc		128.122.88.117	5900	2/19/2020, 7:12:25 AM
Apple remote desktop vnc		128.122.250.47	5900	2/19/2020, 7:11:40 AM
Apple remote desktop vnc		128.122.88.113	5900	2/19/2020, 7:11:26 AM
Apple remote desktop vnc		128.122.88.14	5900	2/19/2020, 7:11:20 AM
Apple remote desktop vnc		128.122.88.15	5900	2/19/2020, 7:11:08 AM
Apple remote desktop vnc		128.122.88.9	5900	2/19/2020, 7:10:56 AM
Apple remote desktop vnc		128.122.110.18	5900	2/19/2020, 7:10:43 AM
VNC		128.122.92.93	5900	2/19/2020, 7:07:36 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		128.122.92.118	5900	2/19/2020, 7:07:34 AM
Apple remote desktop vnc		128.122.86.13	5900	2/19/2020, 7:06:15 AM
VNC		128.122.65.24	5900	2/19/2020, 7:06:14 AM
VNC		128.122.65.230	5900	2/19/2020, 7:03:20 AM
Apple remote desktop vnc		216.165.112.87	5900	2/19/2020, 7:03:02 AM
Apple remote desktop vnc		128.122.110.157	5900	2/19/2020, 6:58:24 AM
Apple remote desktop vnc		128.122.110.56	5900	2/19/2020, 6:57:45 AM
Apple remote desktop vnc		128.122.110.168	5900	2/19/2020, 6:57:25 AM
Apple remote desktop vnc		128.122.95.40	5900	2/19/2020, 6:56:17 AM
Apple remote desktop vnc		128.122.89.186	5900	2/19/2020, 6:55:56 AM
Apple remote desktop vnc		128.122.28.68	5900	2/19/2020, 6:55:33 AM
Apple remote desktop vnc		128.122.9.33	5900	2/19/2020, 6:52:55 AM
Apple remote desktop vnc		216.165.116.103	5900	2/19/2020, 6:52:01 AM
Apple remote desktop vnc		128.122.52.179	5900	2/19/2020, 6:51:04 AM
Apple remote desktop vnc		128.122.90.50	5900	2/19/2020, 6:49:40 AM
Apple remote desktop vnc		128.122.90.33	5900	2/19/2020, 6:49:24 AM
Apple remote desktop vnc		128.122.90.61	5900	2/19/2020, 6:49:23 AM
Apple remote desktop vnc		128.122.90.118	5900	2/19/2020, 6:49:09 AM
Apple remote desktop vnc		128.122.94.135	5900	2/19/2020, 6:43:00 AM
Apple remote desktop vnc		128.122.71.198	5900	2/19/2020, 6:35:47 AM
Apple remote desktop vnc		216.165.116.59	5900	2/19/2020, 6:34:09 AM
VNC		128.122.133.26	5900	2/19/2020, 6:29:07 AM
Apple remote desktop vnc		128.122.60.191	5900	2/19/2020, 6:24:49 AM
Apple remote desktop vnc		128.122.203.235	5900	2/19/2020, 6:24:42 AM
Apple remote desktop vnc		128.122.60.170	5900	2/19/2020, 6:24:41 AM
Apple remote desktop vnc		128.122.60.136	5900	2/19/2020, 6:23:47 AM
Apple remote desktop vnc		128.122.87.209	5900	2/19/2020, 6:19:34 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		128.122.70.221	5900	2/19/2020, 6:18:22 AM
Apple remote desktop vnc		128.122.87.193	5900	2/19/2020, 6:17:28 AM
Apple remote desktop vnc		128.122.70.220	5900	2/19/2020, 6:17:15 AM
Apple remote desktop vnc		128.122.87.78	5900	2/19/2020, 6:16:38 AM
Apple remote desktop vnc		128.122.141.215	5900	2/19/2020, 6:13:55 AM
Apple remote desktop vnc		128.122.60.186	5900	2/19/2020, 6:13:22 AM
Apple remote desktop vnc		128.122.185.20	5900	2/19/2020, 6:12:45 AM
Apple remote desktop vnc		128.122.68.232	5900	2/19/2020, 6:03:26 AM
Apple remote desktop vnc		128.122.45.79	5900	2/19/2020, 6:00:34 AM
Apple remote desktop vnc		128.122.45.232	5900	2/19/2020, 5:59:52 AM
Apple remote desktop vnc		128.122.45.153	5900	2/19/2020, 5:59:17 AM
Apple remote desktop vnc		128.122.45.111	5900	2/19/2020, 5:58:57 AM
Apple remote desktop vnc		128.122.250.33	5900	2/19/2020, 5:57:31 AM
Apple remote desktop vnc		128.122.251.13	5900	2/19/2020, 5:56:23 AM
Apple remote desktop vnc		128.122.90188	5900	2/19/2020, 5:55:55 AM
Apple remote desktop vnc		128.122.115.107	5900	2/19/2020, 5:55:35 AM
Apple remote desktop vnc		128.122.115.198	5900	2/19/2020, 5:55:25 AM
Apple remote desktop vnc		128.122.161.197	5900	2/19/2020, 5:52:44 AM
Apple remote desktop vnc		128.122.31.114	5900	2/19/2020, 5:52:06 AM
Apple remote desktop vnc		128.122.161.160	5900	2/19/2020, 5:51:48 AM
Apple remote desktop vnc		128.122.31.62	5900	2/19/2020, 5:51:21 AM
Apple remote desktop vnc		128.122.161.150	5900	2/19/2020, 5:51:00 AM
Apple remote desktop vnc		128.122.100.101	5900	2/19/2020, 5:47:56 AM
Apple remote desktop vnc		216.165.21.1	5900	2/19/2020, 5:47:05 AM
Apple remote desktop vnc		128.122.70.215	5900	2/19/2020, 5:46:43 AM
Apple remote desktop vnc		128.122.70.170	5900	2/19/2020, 5:46:33 AM
Apple remote desktop vnc		128.122.70.173	5900	2/19/2020, 5:46:04 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

Product Name	Product Version	IP Address	Port	Last Observed
Apple remote desktop vnc		128.122.9.37	5900	2/19/2020, 5:38:51 AM
Apple remote desktop vnc		128.122.30.8	5900	2/19/2020, 5:36:55 AM
Apple remote desktop vnc		128.122.30.5	5900	2/19/2020, 5:35:50 AM
VNC		128.122.33.25	5900	2/19/2020, 5:30:25 AM
Apple remote desktop vnc		128.122.37.66	5900	2/19/2020, 5:24:41 AM
Apple remote desktop vnc		128.122.61.56	5900	2/19/2020, 5:22:51 AM
Apple remote desktop vnc		128.122.100.21	5900	2/19/2020, 5:15:08 AM
Apple remote desktop vnc		128.122.201.156	5900	2/19/2020, 5:11:55 AM
Apple remote desktop vnc		128.122.210.15	5900	2/19/2020, 5:10:41 AM
Apple remote desktop vnc		128.122.100.11	5900	2/19/2020, 4:58:06 AM
Apple remote desktop vnc		128.122.44.94	5900	2/19/2020, 4:56:28 AM
Apple remote desktop vnc		128.122.182.254	5900	2/19/2020, 4:54:28 AM
Apple remote desktop vnc		128.122.34.210	5900	2/19/2020, 4:50:55 AM
Apple remote desktop vnc		128.122.31.105	5900	2/19/2020, 4:50:24 AM
Apple remote desktop vnc		128.122.31.67	5900	2/19/2020, 4:49:58 AM
Apple remote desktop vnc		128.122.31.66	5900	2/19/2020, 4:49:40 AM
Apple remote desktop vnc		128.122.31.118	5900	2/19/2020, 4:49:09 AM
VNC		216.165.117.207	5900	2/19/2020, 4:45:53 AM

## !!! Certificate Is Revoked

-0.6 SCORE IMPACT

Revoked certificates prevent TLS clients from connecting to servers.

### Description

When a Certificate Authority (CA) issues a certificate, they embed URLs that can be visited to check if a certificate has been revoked. Certificates that are revoked are no longer valid, and TLS clients will refuse to connect to servers presenting revoked certificates. Certificates are revoked for a variety of reasons: the decommissioning of a server, the retiring of a product or business name, the early renewal of a certificate, or the belief that an attacker may have acquired the certificate's corresponding private key. The presence of a revoked certificate on the Internet is an indication of an organization either lacking or not adhering to a certificate management policy, or the organization having experienced a breach that has not been fully remediated.

### Recommendation

Generate a new Certificate Signing Request and contact the certificate authority to sign and issue a new certificate.

## 2 findings

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
google.nyu.edu	COMODO CA Limited	216.165.84.74	443	3/6/2020, 5:33:03 AM
google.nyu.edu	COMODO CA Limited	128.122.109.58	443	3/6/2020, 3:09:33 AM

**! Telnet Service Observed**

-&lt;0.1 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.

## 16 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Cisco IOS telnetd	128.238.75.1	23	3/5/2020, 8:59:54 AM
Cisco router telnetd	128.238.14.4	23	3/5/2020, 8:35:01 AM
Cisco router telnetd	128.238.60.10	23	3/5/2020, 7:55:34 AM
Cisco IOS telnetd	128.238.28.41	23	3/5/2020, 7:53:54 AM
Ricoh maintenance telnetd	128.122.8.203	23	3/5/2020, 12:39:29 AM
Polycom ViewStation Video Conferencing telnetd	128.122.180.71	23	3/5/2020, 12:37:32 AM
Linux telnetd	128.122.228.195	23	3/5/2020, 12:15:13 AM
	128.122.2.28	23	3/4/2020, 11:18:18 PM
HP JetDirect telnetd	128.122.185.212	23	3/4/2020, 10:49:45 PM
Polycom ViewStation Video Conferencing telnetd	128.122.19.18	23	3/4/2020, 10:45:45 PM
Cisco router telnetd	216.165.101.2	23	3/4/2020, 8:30:34 PM
BusyBox telnetd	216.165.117.93	23	3/4/2020, 7:20:30 PM
APC PDU/UPS devices or Windows CE telnetd	128.122.71.176	23	3/4/2020, 6:42:42 PM
APC PDU/UPS devices or Windows CE telnetd	128.122.71.177	23	3/4/2020, 6:40:13 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Brother/HP printer telnetd	128.122.63.8	23	2/5/2020, 7:19:45 PM
Linux telnetd	216.165.112.122	23	2/5/2020, 1:34:40 PM

## !! SMB Service Observed

-0.1 SCORE IMPACT

We observed SMB, a file and printer-sharing service, publicly exposed.

### Description

The SMB protocol offers access to files, printers, and other services on a network. We observed an SMB service on the Internet, accessible by the public. These services are attractive targets to attackers due to the data they may contain, and the potential for access to other network resources. 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.

2 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Microsoft Windows 7 - 10 microsoft-ds	128.238.26.20	445	3/10/2020, 11:29:13 PM
Microsoft Windows netbios-ssn	128.238.26.20	139	3/8/2020, 4:48:56 PM

## ✓ TLS Certificate Status Request ("OCSP Stapling") Detected

The organization has taken additional steps to include revocation information with their TLS Certificate response.

### Description

Historically, Certificate Revocation Lists (CRLs) have been the mechanism by which clients can verify the revocation status of a TLS certificate. There are a number of disadvantages to this method including the need for additional network resources from both the clients and servers and the need for libraries to parse these CRLs. Online Certificate Status Protocol (OCSP) was introduced as a lightweight alternative to CRLs. While an OCSP response contains less data than a CRL and is easier to parse, addressing some of the concerns with CRLs, it nevertheless requires clients to make an additional request to verify revocation for every TLS handshake performed. As such, the most common TLS Clients, Web Browsers, do not typically check revocation status of TLS certificates. OCSP stapling, formally known as the TLS Certificate Status Request extension, consists of appending (stapling) the relevant OCSP response to the TLS Handshake, thereby embedding any

### Recommendation

There are no drawbacks to implementing OCSP stapling and servers should adopt this practice wherever possible. In addition to providing clear security benefits, implementation of OCSP stapling removes the need for maintenance of CRLs and can vastly reduce the traffic on organization-owned OCSP servers, which also provides operational benefits.

relevant revocation data without the need for additional network transactions. This provides an overall improvement in security by allowing clients to easily verify revocation information of certificates they receive with minimal operational burden.

## 51 findings

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.35.237	8443	3/11/2020, 1:31:37 AM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.39.237	8443	3/10/2020, 11:56:28 PM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.36.237	8443	3/10/2020, 5:35:43 PM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.38.237	8443	3/10/2020, 5:33:17 PM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.37.237	8443	3/10/2020, 3:39:53 PM
apps-dev.stern.nyu.edu	Internet2	128.122.130.51	443	3/8/2020, 2:38:31 AM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.36.237	443	3/7/2020, 11:21:32 PM
berlin.print.nyu.edu	Internet2	193.175.54.161	443	3/7/2020, 5:57:58 PM
vpn.library.nyu.edu	Internet2	128.122.149.33	443	3/7/2020, 3:59:23 PM
*.law.nyu.edu	Internet2	128.122.51.74	443	3/7/2020, 1:47:06 PM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.38.237	443	3/7/2020, 7:53:26 AM
dagsdc01.shc.sa.nyu.edu	Internet2	128.122.105.10	443	3/7/2020, 6:22:51 AM
mars.nyu.edu	Internet2	128.122.48.182	443	3/7/2020, 6:10:45 AM
mars.nyu.edu	Internet2	128.122.48.181	443	3/7/2020, 6:01:34 AM
its.law.nyu.edu	Internet2	128.122.159.246	443	3/7/2020, 3:11:31 AM
engineering.nyu.edu	s Encrypt	35.172.89.115	443	3/7/2020, 1:55:16 AM
reform.bio.nyu.edu	Internet2	128.122.4.76	443	3/7/2020, 12:25:39 AM
ssl714082.cloudflaressl.com	COMODO CA Limited	104.16.37.237	443	3/6/2020, 11:50:56 PM
research.seed.law.nyu.edu	Internet2	128.122.159.40	443	3/6/2020, 10:44:38 PM
mobileprint.nyu.edu	Internet2	128.122.121.219	443	3/6/2020, 5:50:05 PM
*.nyuad-artscenter.org	Internet2	52.220.171.78	443	3/6/2020, 3:45:24 PM
sofie.stern.nyu.edu	s Encrypt	128.122.85.97	443	3/6/2020, 11:04:18 AM
vclqa.home.nyu.edu	Internet2	128.122.120.77	443	3/6/2020, 7:45:08 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
tstcfm.law.nyu.edu	Internet2	128.122.51.34	443	3/6/2020, 4:02:20 AM
*.law.nyu.edu	Internet2	128.122.51.75	443	3/6/2020, 4:01:33 AM
its.law.nyu.edu	Internet2	128.122.51.85	443	3/6/2020, 3:58:19 AM
listservpublic.med.nyu.edu	DigiCert Inc	216.165.125.130	443	3/5/2020, 11:03:27 PM
orion.stern.nyu.edu	Internet2	128.122.130.193	443	3/5/2020, 5:10:29 PM
cslc.nursing.nyu.edu	Internet2	128.122.174.6	443	3/5/2020, 5:02:44 PM
apps-dev.stern.nyu.edu	Internet2	128.122.130.90	443	3/5/2020, 4:52:43 PM
*.law.nyu.edu	Internet2	128.122.159.99	443	3/5/2020, 4:46:10 PM
*.law.nyu.edu	Internet2	128.122.159.101	443	3/5/2020, 4:38:49 PM
vpn.library.nyu.edu	Internet2	128.122.149.225	443	3/5/2020, 5:32:29 AM
coi.nyu.edu	Internet2	128.122.209.96	443	3/5/2020, 5:28:15 AM
ill.library.nyu.edu	Internet2	128.122.149.45	443	3/5/2020, 5:11:10 AM
*.nyuad-artscenter.org	Internet2	52.220.171.155	443	3/5/2020, 1:15:28 AM
orientation.sps.nyu.edu	Internet2	173.224.73.240	443	3/5/2020, 12:04:16 AM
mail.nyumc.org	DigiCert Inc	216.165.125.29	443	3/4/2020, 6:01:35 PM
kop003-wwb-tv.cfs.its.nyu.edu	Internet2	128.122.121.103	443	3/4/2020, 5:41:46 PM
apps-ng.stern.nyu.edu	Internet2	128.122.130.105	443	2/8/2020, 10:47:10 PM
mail.nyumc.org	DigiCert Inc	47.19.237.154	443	2/8/2020, 4:45:56 PM
vpn.library.nyu.edu	Internet2	128.122.149.24	443	2/8/2020, 12:05:46 PM
cccw.it.ed.nyu.edu	Internet2	128.122.30.30	443	2/8/2020, 7:54:56 AM
itp.nyu.edu	Internet2	128.122.120.76	443	2/8/2020, 7:45:00 AM
shcportal.nyu.edu	Internet2	128.122.104.214	443	2/8/2020, 2:42:34 AM
csdportal.nyu.edu	Internet2	128.122.104.192	443	2/7/2020, 6:35:25 AM
*.law.nyu.edu	Internet2	128.122.51.45	443	2/7/2020, 12:56:10 AM
kimmelonestop.nyu.edu	Internet2	128.122.121.31	443	2/6/2020, 7:38:00 PM
ssswforms.ssw.nyu.edu	Internet2	128.122.123.52	443	2/6/2020, 9:19:57 AM
winterm-p1.stern.nyu.edu	Internet2	128.122.130.11	443	2/6/2020, 5:30:54 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
ogsonline.ogs.nyu.edu	Internet2	128.122.122.131	443	2/6/2020, 12:31:14 AM

## !! MySQL Service Observed

-0.4 SCORE IMPACT

We observed MySQL, a database management system, publicly exposed.

### Description

MySQL is an open-source database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a MySQL service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database 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 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.

### Recommendation

Exposing database 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 whitelisting the IP addresses that require access.

### 33 findings

PRODUCT NAME	PRODUCT VERSION	IP ADDRESS	PORT	LAST OBSERVED
MySQL	5.1.39	128.238.66.55	3306	2/20/2020, 12:27:00 PM
MySQL	5.5.30	70.32.92.51	3306	2/20/2020, 11:54:20 AM
MySQL	5.6.46-cll-lve	107.180.61.237	3306	2/20/2020, 11:08:47 AM
MySQL		159.65.160.172	3306	2/20/2020, 9:30:03 AM
MySQL	5.5.64-MariaDB	128.122.85.51	3306	2/16/2020, 3:42:58 PM
MySQL	5.6.21	128.122.136.97	3306	2/16/2020, 3:20:45 PM
MySQL		128.122.102.203	3306	2/16/2020, 3:09:58 PM
MySQL		128.122.2.189	3306	2/16/2020, 3:08:34 PM
MySQL		128.122.179.183	3306	2/16/2020, 3:01:53 PM
MySQL		128.122.201.108	3306	2/16/2020, 2:53:40 PM
MySQL		128.122.115.147	3306	2/16/2020, 2:37:09 PM
MySQL		128.122.141.55	3306	2/16/2020, 2:26:02 PM

Product Name	Product Version	IP Address	Port	Last Observed
MariaDB		128.122.141.21	3306	2/16/2020, 2:20:23 PM
MySQL		128.122.112.94	3306	2/16/2020, 2:09:58 PM
MariaDB		128.122.33.16	3306	2/16/2020, 1:41:45 PM
MariaDB		128.122.251.184	3306	2/16/2020, 1:38:48 PM
MySQL	5.7.27-0ubuntu0.16.04.1	128.122.34.202	3306	2/16/2020, 1:35:30 PM
MySQL	5.5.5-10.4.6-MariaDB	128.122.28.118	3306	2/16/2020, 1:33:17 PM
MySQL	5.6.33-0ubuntu0.14.04.1~es7-log	128.122.161.15	3306	2/16/2020, 1:19:44 PM
MySQL		128.122.136.78	3306	2/16/2020, 12:59:46 PM
MySQL		128.122.90.172	3306	2/16/2020, 12:47:02 PM
MySQL	5.7.16-log	216.165.117.236	3306	2/16/2020, 12:01:08 PM
MySQL		128.122.235.5	3306	2/16/2020, 11:34:11 AM
MySQL		128.122.131.35	3306	2/16/2020, 10:27:51 AM
MariaDB		128.122.136.17	3306	2/16/2020, 10:13:18 AM
MySQL		128.122.70.174	3306	2/16/2020, 9:40:49 AM
MySQL		128.122.250.33	3306	2/16/2020, 8:59:00 AM
MySQL		216.165.21.1	3306	2/16/2020, 8:37:56 AM
MySQL	5.7.11-log	128.122.30.11	3306	2/16/2020, 8:17:25 AM
MySQL		128.122.100.101	3306	2/16/2020, 8:14:10 AM
MySQL	5.7.26-0ubuntu0.16.04.1	128.122.180.39	3306	2/16/2020, 7:57:10 AM
MySQL	5.5.5-10.1.35-MariaDB	128.122.224.5	3306	2/16/2020, 7:24:15 AM
MySQL	5.6.47	128.122.85.21	3306	2/16/2020, 7:13:57 AM

## !! SSH Supports Weak MAC

-0.3 SCORE IMPACT

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

### Description

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.

### Recommendation

Configure the SSH server to disable the use of MD5.

## 109 findings

IP ADDRESS	PORT	LAST OBSERVED
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : hmac-md5		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : hmac-md5-96		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : hmac-md5-eth@openssh.com		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : hmac-md5		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : hmac-md5-96		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : hmac-md5-96-eth@openssh.com		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : hmac-md5		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : hmac-md5-96		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : hmac-md5-96		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : hmac-md5		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : hmac-md5-96		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : hmac-md5		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : hmac-md5		
128.238.66.31	22	2/12/2020, 3:04:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : hmac-md5		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : hmac-md5-96		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : hmac-md5-96		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : hmac-md5		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : hmac-md5-utm@openssh.com		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : hmac-md5		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : hmac-md5-96		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : hmac-md5-96		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : hmac-md5		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : hmac-md5		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : hmac-md5-utm@openssh.com		
128.238.147.222	22	2/12/2020, 2:55:06 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : hmac-md5-96		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : hmac-md5-96-utm@openssh.com		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : hmac-md5		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : hmac-md5-96		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : hmac-md5		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : hmac-md5-96		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : hmac-md5		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : hmac-md5-96		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : hmac-md5		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : hmac-md5-96		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : hmac-md5		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.147.215	22	2/12/2020, 2:16:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : hmac-md5		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : hmac-md5-utm@openssh.com		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : hmac-md5		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : hmac-md5-96		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : hmac-md5-utm@openssh.com		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : hmac-md5-96-utm@openssh.com		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : hmac-md5-96		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : hmac-md5		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : hmac-md5-utm@openssh.com		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : hmac-md5		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : hmac-md5-96		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : hmac-md5		
195.113.94.147	22	2/12/2020, 1:48:19 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : hmac-md5		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : hmac-md5-96		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : hmac-md5-96		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : hmac-md5		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : hmac-md5		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : hmac-md5-96		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : hmac-md5-96@openssh.com		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : hmac-md5-96		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : hmac-md5		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : hmac-md5-96-96@openssh.com		
128.238.118.20	22	2/12/2020, 1:11:45 PM
Evidence : hmac-md5		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : hmac-md5-96@openssh.com		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : hmac-md5		
128.238.147.230	22	2/12/2020, 1:00:53 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96-etm@openssh.com		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : hmac-md5-96		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : hmac-md5-96		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : hmac-md5		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : hmac-md5		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : hmac-md5-96		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : hmac-md5		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : hmac-md5-96-etm@openssh.com		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : hmac-md5-96		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : hmac-md5-etm@openssh.com		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : hmac-md5-96		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : hmac-md5		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : hmac-md5-96-etm@openssh.com		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : hmac-md5-96-etm@openssh.com		
128.238.75.1	22	2/12/2020, 12:30:35 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
128.238.75.1	22	2/12/2020, 12:30:35 PM
Evidence : hmac-md5		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : hmac-md5		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : hmac-md5-96		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : hmac-md5		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : hmac-md5-96@openssh.com		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : hmac-md5		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : hmac-md5-96@openssh.com		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : hmac-md5		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : hmac-md5		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : hmac-md5-96		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : hmac-md5		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : hmac-md5-96@openssh.com		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : hmac-md5		
45.55.130.164	22	2/12/2020, 11:48:33 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : hmac-md5-96		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : hmac-md5-96-utm@openssh.com		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : hmac-md5		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : hmac-md5-96		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : hmac-md5		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : hmac-md5-96		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : hmac-md5		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : hmac-md5-96-utm@openssh.com		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : hmac-md5-utm@openssh.com		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : hmac-md5-96		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : hmac-md5		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : hmac-md5-96		

## !! RDP Service Observed

-0.2 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

### 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

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.

possible, restrict the service by whitelisting the IP addresses that require access.

## 10 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Microsoft Terminal Services	128.238.38.63	3389	2/26/2020, 4:54:20 PM
Microsoft Terminal Services	18.221.167.13	3389	2/26/2020, 4:50:11 PM
Microsoft Terminal Services	128.238.118.30	3389	2/26/2020, 4:44:02 PM
Microsoft Terminal Services	128.238.118.26	3389	2/26/2020, 4:31:39 PM
Microsoft Terminal Services	128.238.26.20	3389	2/26/2020, 4:12:30 PM
Microsoft Terminal Services	80.250.25.114	3389	2/26/2020, 4:05:32 PM
Microsoft Terminal Services	128.238.38.4	3389	2/26/2020, 3:46:08 PM
Microsoft Terminal Services	128.238.38.62	3389	2/26/2020, 3:44:03 PM
Microsoft Terminal Services	128.238.184.105	3389	2/26/2020, 3:41:24 PM
Microsoft Terminal Services	128.238.1.39	3389	2/21/2020, 10:21:17 PM

## !! TLS Protocol Uses Weak Cipher

-0.7 SCORE IMPACT

TLS analysis reveals a weak cipher either through encryption protocol or public key length.

### Description

The TLS cryptographic configuration being used could be defeated. A symmetric cipher suite is specified by an encryption protocol (e.g. DES, AES). The strength of the encryption used within a Transport Layer Security (TLS) session is determined by the encryption symmetric cipher negotiated between the server and the browser. In order to ensure that only strong cryptographic ciphers are selected the server must be modified to disable the use of weak ciphers and to configure the ciphers in an adequate order. Additionally, as part of the TLS handshake, an asymmetric cipher is utilized. The strength of the asymmetric cipher may be weakened if an insufficient key size is selected.

### Recommendation

It is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.

## 82 findings

CERTIFICATE COMMON NAME	COLLECTION TARGET	PORT	LAST OBSERVED
api.nyu.edu	34.237.231.189	443	3/11/2020, 10:35:38 PM
intake24.abudhabi.nyu.edu	91.230.41.40	443	3/11/2020, 9:44:02 PM
events.shanghai.nyu.edu	13.231.227.172	443	3/11/2020, 4:28:46 PM
xbnews.abudhabi.nyu.edu	91.230.41.26	443	3/11/2020, 3:59:13 PM
sandbox.api.it.nyu.edu	35.169.42.80	443	3/11/2020, 1:52:14 PM
token.idm.home.nyu.edu	34.231.72.14	443	3/11/2020, 1:31:28 PM
maps-public.geo.nyu.edu	52.3.70.94	443	3/11/2020, 7:38:02 AM
devitwikis.nyu.edu	199.119.125.133	443	3/11/2020, 7:15:13 AM
ssl714082.cloudflaressl.com	104.16.35.237	8443	3/11/2020, 1:31:37 AM
ssl714082.cloudflaressl.com	104.16.39.237	8443	3/10/2020, 11:56:28 PM
spark.stern.nyu.edu	107.22.255.58	443	3/10/2020, 10:05:28 PM
giRFUjeGvcwauUmQuEfuixyiagIluKn aJLwxrFL.nyu.edu	64.227.10.175	443	3/10/2020, 9:54:45 PM
ssl714082.cloudflaressl.com	104.16.36.237	8443	3/10/2020, 5:35:43 PM
ssl714082.cloudflaressl.com	104.16.38.237	8443	3/10/2020, 5:33:17 PM
ssl714082.cloudflaressl.com	104.16.37.237	8443	3/10/2020, 3:39:53 PM
mail.bottou.org	216.165.22.6	995	3/10/2020, 7:56:09 AM
mail.bottou.org	216.165.22.6	993	3/9/2020, 10:46:27 PM
*.med.nyu.edu	216.165.125.215	443	3/8/2020, 2:46:58 AM
w4-test.stern.nyu.edu	128.122.130.6	443	3/8/2020, 2:44:16 AM
w4.stern.nyu.edu	128.122.130.29	443	3/8/2020, 2:35:34 AM
dev-sites.dlib.nyu.edu	128.122.108.64	443	3/8/2020, 2:13:05 AM
ssl714082.cloudflaressl.com	104.16.36.237	443	3/7/2020, 11:21:32 PM
datepalmgenomehub.abudhabi.ny. edu	91.230.41.11	443	3/7/2020, 10:19:14 PM
secure-usea1- 1.tessituranetwork.com	54.173.20.118	443	3/7/2020, 6:59:46 PM
cds1.cvent.com	192.190.92.31	443	3/7/2020, 4:16:50 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	COLLECTION TARGET	PORT	LAST OBSERVED
web1.library.nyu.edu	128.122.149.60	443	3/7/2020, 3:53:00 PM
ssl714082.cloudflare.com	104.16.38.237	443	3/7/2020, 7:53:26 AM
www.nyu.edu	52.196.207.156	443	3/7/2020, 4:07:22 AM
isaw.nyu.edu	66.35.48.30	443	3/7/2020, 4:06:17 AM
ldcsa.shanghai.nyu.edu	180.168.176.129	443	3/7/2020, 2:24:51 AM
engineering.nyu.edu	35.172.89.115	443	3/7/2020, 1:55:16 AM
rh.abudhabi.nyu.edu	91.230.41.37	443	3/7/2020, 1:34:53 AM
*.leoyan.com	216.165.22.6	443	3/7/2020, 1:21:51 AM
ssl714082.cloudflare.com	104.16.37.237	443	3/6/2020, 11:50:56 PM
secure-usea1-1.tessituranetwork.com	34.199.219.24	443	3/6/2020, 10:05:04 PM
vgc.poly.edu	128.238.182.100	443	3/6/2020, 9:49:36 PM
redcap.bio.nyu.edu	128.122.4.29	443	3/6/2020, 9:38:26 PM
qaauth.home.nyu.edu	216.165.49.17	443	3/6/2020, 9:08:22 PM
jbrowsephoenix.abudhabi.nyu.edu	91.230.41.217	443	3/6/2020, 8:45:16 PM
candidates.admission.shanghai.nyu.edu	107.22.237.69	443	3/6/2020, 7:26:24 PM
lb03.pacloud.com	198.101.168.201	443	3/6/2020, 5:16:02 PM
www.bookstores.nyu.edu	128.122.37.209	443	3/6/2020, 5:08:56 PM
compliance.report.shanghai.nyu.edu	59.79.127.54	443	3/6/2020, 4:53:36 PM
code.engineering.nyu.edu	128.238.63.88	443	3/6/2020, 1:53:12 PM
secure-usea1-1.tessituranetwork.com	72.29.126.235	443	3/6/2020, 8:29:28 AM
library.nyu.edu	34.192.16.97	443	3/6/2020, 7:49:32 AM
secure-usea1-1.tessituranetwork.com	72.29.98.156	443	3/6/2020, 6:09:05 AM
secure-usea1-1.tessituranetwork.com	72.29.98.167	443	3/6/2020, 6:05:00 AM
uathercules.home.nyu.edu	216.165.48.17	443	3/6/2020, 5:07:17 AM
qanewhome.home.nyu.edu	216.165.49.21	443	3/6/2020, 3:28:13 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	COLLECTION TARGET	PORT	LAST OBSERVED
secure-usea1-1.tessituranetwork.com	54.236.165.210	443	3/6/2020, 2:17:06 AM
holostor.hpc.nyu.edu	128.122.215.23	443	3/6/2020, 1:55:25 AM
hyper.ifa.nyu.edu	128.122.65.146	443	3/6/2020, 1:29:31 AM
secure-usea1-1.tessituranetwork.com	54.156.167.203	443	3/6/2020, 12:45:12 AM
stu.itp.nyu.edu	128.122.157.182	443	3/5/2020, 11:39:27 PM
physics.nyu.edu	216.165.26.109	443	3/5/2020, 11:34:43 PM
mail.nyumc.org	216.165.125.175	443	3/5/2020, 11:07:40 PM
*.med.nyu.edu	216.165.125.141	443	3/5/2020, 10:57:38 PM
*.med.nyu.edu	216.165.125.110	443	3/5/2020, 10:54:30 PM
*.med.nyu.edu	216.165.125.108	443	3/5/2020, 10:50:28 PM
www.nyu.edu	52.198.45.18	443	3/5/2020, 10:20:58 PM
online.engineering.nyu.edu	52.0.197.6	443	3/5/2020, 10:02:04 PM
secure-usea1-1.tessituranetwork.com	72.29.98.163	443	3/5/2020, 8:42:46 PM
sandboxclasses1.home.nyu.edu	216.165.48.14	443	3/5/2020, 8:39:15 PM
horatio.cs.nyu.edu	216.165.22.17	443	3/5/2020, 7:40:57 PM
ais.stern.nyu.edu	128.122.130.25	443	3/5/2020, 5:07:42 PM
apps-dev.stern.nyu.edu	128.122.130.189	443	3/5/2020, 5:06:26 PM
clame.nyu.edu	66.228.45.202	443	3/5/2020, 1:47:16 PM
engineering.nyu.edu	52.4.249.152	443	3/5/2020, 9:27:19 AM
Plumix.com	91.205.174.26	443	3/5/2020, 7:30:46 AM
mail.nyumc.org	47.19.237.172	443	3/5/2020, 6:36:29 AM
mail.nyumc.org	47.19.237.152	443	3/5/2020, 6:32:44 AM
rooms.library.nyu.edu	128.122.149.134	443	3/5/2020, 5:17:44 AM
*.getit.library.nyu.edu	128.122.149.164	443	3/5/2020, 5:16:46 AM
pdsdev.library.nyu.edu	128.122.149.82	443	3/5/2020, 5:10:28 AM
*.nyuad-artscenter.org	52.220.171.155	443	3/5/2020, 1:15:28 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	COLLECTION TARGET	PORT	LAST OBSERVED
engineering.nyu.edu	54.209.255.182	443	3/4/2020, 9:53:40 PM
www.nyu.edu	216.165.85.208	443	3/4/2020, 9:26:43 PM
*.med.nyu.edu	4719.237.150	443	3/4/2020, 8:07:13 PM
cic.nyu.edu	128.122.109.30	443	3/4/2020, 7:31:00 PM
mail.nyumc.org	216.165.125.29	443	3/4/2020, 6:01:35 PM
berlin-ib.berlin.nyu.edu	193.175.54.7	443	3/4/2020, 5:57:05 PM

## i POP3 Service Observed

We observed POP3, an email retrieval service, publicly exposed.

### Description

The POP3 protocol offers access to messages stored on email servers. POP3 servers typically contain only the most recent messages received by an email account, deleting the messages from the server once they are downloaded by a user. The use of POP3 may complicate BCP/DR due to each individual user being responsible for the entirety of their email history. We observed a POP3 service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. 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 access the messages within. 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.

### Recommendation

Review the business necessity of hosting a public POP3 server, and remove it from the Internet if possible. If not possible, consider restricting the service by whitelisting the IP addresses that require access.

## 28 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Dovecot pop3d	37.60.232.214	110	3/8/2020, 6:14:00 AM
Dovecot pop3d	128.122.205.35	110	3/8/2020, 6:07:53 AM
Dovecot pop3d	128.122.49.90	110	3/8/2020, 5:01:30 AM
Dovecot pop3d	128.122.49.91	110	3/8/2020, 4:59:39 AM
Dovecot pop3d	107.180.61.237	110	3/8/2020, 4:42:12 AM

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Courier pop3d	70.32.92.51	110	3/8/2020, 4:30:20 AM
Dovecot pop3d	70.32.96.242	110	3/8/2020, 2:30:16 AM
Dovecot pop3d	128.122.87.78	110	3/8/2020, 2:06:28 AM
Dovecot pop3d	128.122.253.9	110	3/8/2020, 1:04:52 AM
Dovecot pop3d	35.214.191.115	110	3/8/2020, 12:47:59 AM
Dovecot pop3d	159.65.160.172	1900	3/2/2020, 9:58:43 PM
Dovecot pop3d	159.65.160.172	5900	2/28/2020, 2:15:39 PM
Dovecot pop3d	159.65.160.172	1089	2/18/2020, 3:48:50 AM
Dovecot pop3d	128.122.87.78	995	2/14/2020, 4:13:05 PM
Dovecot pop3d	159.65.160.172	37	2/14/2020, 3:57:17 PM
Dovecot pop3d	128.122.49.90	995	2/14/2020, 3:33:42 PM
Dovecot pop3d	128.122.205.35	995	2/14/2020, 2:52:13 PM
Dovecot pop3d	35.214.191.115	995	2/14/2020, 2:38:30 PM
Dovecot pop3d	70.32.96.242	995	2/14/2020, 2:11:25 PM
Dovecot pop3d	128.122.253.9	995	2/14/2020, 2:03:29 PM
Dovecot pop3d	37.60.232.214	995	2/14/2020, 11:58:41 AM
Courier pop3d	70.32.92.51	995	2/14/2020, 11:46:16 AM
Dovecot pop3d	107.180.61.237	995	2/14/2020, 11:13:44 AM
Dovecot pop3d	128.122.49.91	995	2/14/2020, 11:03:39 AM
Dovecot pop3d	159.65.160.172	5000	2/8/2020, 3:40:41 PM
Dovecot pop3d	159.65.160.172	79	2/7/2020, 11:20:26 AM
Dovecot pop3d	159.65.160.172	990	2/6/2020, 6:32:15 PM
Dovecot pop3d	159.65.160.172	139	2/6/2020, 4:23:11 PM

## !! rsync Service Observed

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

-0.3 SCORE IMPACT

**Description**

The rsync protocol provides an efficient method of transferring files between hosts. The rsync service offers access to files stored on servers, giving users the ability to upload, download, and delete files. The rsync daemon does not support encryption, exposing all uploaded and downloaded files to man-in-the-middle attacks. We observed an rsync daemon 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 rsync server may sell the files within, use them for blackmail, or employ the information when launching further attacks. A breached rsync 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 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.

**Recommendation**

Exposing rsync 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 whitelisting the IP addresses that require access.

**5 findings**

IP ADDRESS	PORT	LAST OBSERVED
128.122.133.17	873	2/13/2020, 7:27:34 PM
128.122.65.62	873	2/13/2020, 7:18:26 PM
128.122.133.16	873	2/13/2020, 6:12:49 PM
128.122.161.15	873	2/13/2020, 6:07:23 PM
128.122.109.46	873	2/13/2020, 6:00:20 PM

**! TLS Certificate Without Revocation Control**

**-0.2** SCORE IMPACT

We observed a TLS certificate that did not contain either CRL or OCSP URLs.

**Description**

Certificate revocation lists (CRLs) are files published online by certificate authorities (CAs). These lists indicate which certificates the CA has revoked, invalidating those certificates. TLS clients (e.g., web browsers) may download a CRL, referenced by a TLS server's certificate, to confirm the certificate is currently valid. CAs may operate online certificate status protocol (OCSP) servers, allowing TLS clients to query whether a certificate is currently valid. Responses to OCSP queries may be 'stapled to' (bundled with) certificates by TLS servers. OCSP stapling prevents TLS clients from needing to query the OCSP server themselves, resulting in faster TLS connections. If an attacker acquires the private key corresponding to a certificate, or any other breach of the private key occurs, the CA can use the revocation controls described above to inform TLS clients that the certificate is no longer valid. Certificates that do not contain revocation

**Recommendation**

Contact the CA to request that the certificate be reissued with revocation controls.

controls cannot be revoked, and if an attacker acquires the certificate's private key then the certificate will be valid until the expiry date.

## 55 findings

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
dev.spacecheckin.nyu.edu	Internet2	34.194.100.20	443	3/11/2020, 11:20:47 PM
vpn.florence.nyu.edu	Internet2	193.205.158.43	443	3/11/2020, 7:40:34 PM
sandbox.api.it.nyu.edu	Internet2	35.169.42.80	443	3/11/2020, 1:52:14 PM
login.k8s-web-dev.library.nyu.edu	NYU	34.231.224.146	443	3/11/2020, 4:52:43 AM
arch.library.nyu.edu	Internet2	34.194.159.248	443	3/11/2020, 1:35:18 AM
login.k8s-web-prod.library.nyu.edu	NYU	34.227.62.91	443	3/11/2020, 1:13:34 AM
src-server1.sl.sa.nyu.edu	New York University - SRC	128.122.110.168	8443	3/10/2020, 11:01:47 PM
giRFUjeGvcwauUmQuEfuixyi aglliuknaJLwxrFL.nyu.edu	SomeOrganization	64.227.10.175	443	3/10/2020, 9:54:45 PM
ronan.ad.law.nyu.edu	Symantec Corporation	128.122.159.7	8443	3/10/2020, 12:13:14 PM
motordocs.psych.nyu.edu	NYU Infant Action Lab	128.122.87.78	995	3/10/2020, 4:44:10 AM
fedora1016.chem.nyu.edu	NYU	128.122.250.124	993	3/9/2020, 10:40:30 PM
motordocs.psych.nyu.edu	NYU Infant Action Lab	128.122.87.78	993	3/9/2020, 7:32:20 PM
MERCURY2017.CAREER.AD MIN.NYU.EDU	NYU Wasserman Center	128.122.45.234	636	3/9/2020, 5:29:38 AM
motordocs.psych.nyu.edu	NYU Infant Action Lab	128.122.87.78	636	3/9/2020, 3:27:25 AM
src-server1.sl.sa.nyu.edu	New York University - SRC	128.122.110.168	636	3/9/2020, 2:35:40 AM
HEMISERVER.HEMI.ADMIN. NYU.EDU	Hemispheric Institute	128.122.28.96	636	3/9/2020, 2:23:44 AM
execed-proxy.stern.nyu.edu	New York University	128.122.130.23	443	3/8/2020, 2:45:25 AM
broyde26.bio.nyu.edu	broyde17.bio.nyu.edu	128.122.60.77	443	3/8/2020, 12:11:26 AM
*.apps.nyu-openshift-poc.ocp.it.nyu.edu		34.206.207.200	443	3/7/2020, 9:27:02 AM
NPI0403BD.nyu.edu	Hewlett-Packard Co.	128.122.31.60	443	3/7/2020, 4:09:46 AM
dsswkr2.home.nyu.edu	SomeOrganization	216.165.32.97	443	3/7/2020, 2:14:26 AM

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
*.leoyan.com	Leoyan	216.165.22.6	443	3/7/2020, 1:21:51 AM
cauchy.cns.nyu.edu	New York University	128.122.112.30	443	3/7/2020, 12:40:58 AM
engineering.nyu.edu	SomeOrganization	52.5.55.254	443	3/6/2020, 11:54:45 PM
ftvjss_serverosx.filmtv.tsoa.ny.edu		128.122.102.203	443	3/6/2020, 11:44:00 PM
cue2.engineering.nyu.edu		216.165.117.5	443	3/6/2020, 10:47:01 PM
aquila.bio.nyu.edu	New York University	128.122.4.26	443	3/6/2020, 9:46:54 PM
mc.dlib.nyu.edu	SomeOrganization	128.122.108.91	443	3/6/2020, 6:25:32 PM
*.apps.nyu Openshift-poc.ocp.it.nyu.edu		18.213.213.81	443	3/6/2020, 12:53:41 PM
cue1.engineering.nyu.edu		216.165.116.103	443	3/6/2020, 10:18:49 AM
login.k8s-web-prod.library.nyu.edu	NYU	54.164.219.133	443	3/6/2020, 2:38:19 AM
status.print.nyu.edu	Amazon	34.194.72.5	443	3/5/2020, 8:13:17 PM
horatio.cs.nyu.edu	SomeOrganization	216.165.22.17	443	3/5/2020, 7:40:57 PM
puppet-p1.stern.nyu.edu		128.122.130.133	443	3/5/2020, 4:58:42 PM
ronan.ad.law.nyu.edu	Symantec Corporation	128.122.159.7	443	3/5/2020, 4:48:56 PM
engineering.nyu.edu	SomeOrganization	52.4.249.152	443	3/5/2020, 9:27:19 AM
NPI489A83.nyu.edu	Hewlett-Packard Co.	140.247.89.115	443	3/4/2020, 9:56:22 PM
*.apps.nyu Openshift-poc.ocp.it.nyu.edu		52.6.11.57	443	3/4/2020, 7:21:34 PM
berlin-ib.berlin.nyu.edu	Infoblox	193.175.54.7	443	3/4/2020, 5:57:05 PM
fedora1016.chem.nyu.edu	NYU	128.122.250.124	143	3/4/2020, 11:53:52 AM
*.speech.steinhardt.nyu.edu	Amazon	35.167.243.251	443	3/4/2020, 11:30:29 AM
library.nyu.edu	Internet2	34.192.16.97	443	3/3/2020, 10:01:41 PM
rh.abudhabi.nyu.edu	Internet2	91.230.41.37	443	3/3/2020, 8:57:58 PM
motordocs.psych.nyu.edu	NYU Infant Action Lab	128.122.87.78	110	3/3/2020, 4:45:47 PM
vpn.paris.nyu.edu	Internet2	194.214.81.35	443	3/3/2020, 3:06:38 PM
diploma.sps.nyu.edu	Internet2	107.21.110.124	443	3/3/2020, 1:19:35 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
london-ib.london.nyu.edu	Infoblox	212.219.93.7	443	2/8/2020, 10:20:01 PM
SHCPOLY.nyu.edu	Polycom Inc.	216.165.117.2	443	2/8/2020, 4:06:09 PM
tick.nyu.edu	New York University	128.122.253.8	443	2/7/2020, 5:41:57 PM
login.k8s-web-prod.library.nyu.edu	NYU	34.206.34.17	443	2/7/2020, 1:30:59 PM
POLYCOM.stern.nyu.edu	Polycom Inc.	128.122.180.71	443	2/7/2020, 4:39:44 AM
login.k8s-web-dev.library.nyu.edu	NYU	34.200.38.12	443	2/6/2020, 9:34:42 PM
MERCURY2017.CAREER.AD MIN.NYU.EDU	NYU Wasserman Center	128.122.45.234	443	2/6/2020, 1:00:04 AM
broyde29.bio.nyu.edu	broyde17.bio.nyu.edu	128.122.60.80	443	2/5/2020, 11:59:04 PM
login.k8s-web-dev.library.nyu.edu	NYU	52.202.5.23	443	2/5/2020, 9:58:39 PM

## ! Certificate Lifetime Is Longer Than Best Practices

-0.2 SCORE IMPACT

We observed a certificate with a lifetime longer than 39 Months.

### 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 the certificate a TLS server (e.g., website) presents to a client (e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Cryptographic algorithms do not have a defined lifetime, but academics, researchers, and nation states are constantly evaluating them for weaknesses. New algorithms and versions of algorithms with larger key sizes are created regularly, and the best practices surrounding certificates evolve with them. The Certificate Authority and Browser forum, an industry group that sets standards surrounding the creation and use of certificates, has decided to limit the lifetime of certificates to 39 months. This means that CAs who are members of the forum are required to issue certificates with lifetimes that do not exceed 39 months.

### Recommendation

Contact the CA and arrange the issuance of a new certificate with a lifetime that does not exceed 39 months.

### 12 findings

CERTIFICATE COMMON NAME	START DATE	EXPIRATION DATE	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
ronan.ad.law.nyu.edu	11/22/2017, 5:46:11 PM	12/20/2027, 5:46:11 PM	Symantec Corporation	128.122.159.7	8443	3/10/2020, 12:13:14 PM
broyde26.bio.nyu.edu	1/8/2019, 12:22:48 AM	1/8/2024, 12:22:48 AM	broyde17.bio.nyu.edu	128.122.60.77	443	3/8/2020, 12:11:26 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	START DATE	EXPIRATION DATE	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
NPI0403BD.nyu.edu	12/1/2017, 12:00:00 AM	12/1/2027, 12:00:00 AM	Hewlett-Packard Co.	128.122.31.60	443	3/7/2020, 4:09:46 AM
*.leoyan.com	3/6/2011, 3:37:32 AM	3/3/2021, 3:37:32 AM	Leoyan	216.165.22.6	443	3/7/2020, 1:21:51 AM
ingestion2-sonyc.engineering.nyu.edu	12/19/2016, 12:05:07 PM	10/1/2431, 12:30:33 PM	New York University	128.238.182.12	443	3/6/2020, 4:53:36 PM
ingestion1-sonyc.engineering.nyu.edu	12/19/2016, 12:02:52 PM	10/1/2431, 12:28:18 PM	New York University	128.238.182.11	443	3/6/2020, 5:48:59 AM
puppet-p1.stern.nyu.edu	10/18/2017, 6:29:52 PM	10/18/2022, 6:29:52 PM		128.122.130.133	443	3/5/2020, 4:58:42 PM
ronan.ad.law.nyu.edu	11/22/2017, 5:46:11 PM	12/20/2027, 5:46:11 PM	Symantec Corporation	128.122.159.7	443	3/5/2020, 4:48:56 PM
NPI489A83.nyu.edu	9/1/2016, 12:00:00 AM	9/1/2026, 12:00:00 AM	Hewlett-Packard Co.	140.247.89.115	443	3/4/2020, 9:56:22 PM
SHCPOLY.nyu.edu	8/27/2015, 6:19:17 PM	8/24/2025, 6:19:17 PM	Polycom Inc.	216.165.117.2	443	2/8/2020, 4:06:09 PM
POLYCOM.stern.ny.edu	7/17/2019, 4:49:03 PM	7/14/2029, 4:49:03 PM	Polycom Inc.	128.122.180.71	443	2/7/2020, 4:39:44 AM
broyde29.bio.nyu.edu	1/8/2019, 12:24:56 AM	1/8/2024, 12:24:56 AM	broyde17.bio.nyu.edu	128.122.60.80	443	2/5/2020, 11:59:04 PM

## ✓ Extended Validation Certificate Observed

The organization has undergone an extended identity-validation process when acquiring a certificate.

### Description

Certificate Authorities (CAs) issue certificates according to a variety of policies, and embed within each certificate a reference to the policy under which it was issued. The type of policy that offers the most assurance of the certificate-holder's identity is called an extended validation (EV) policy, and certificates issued under these policies are called EV certificates. To receive an EV certificate, an organization must prove to a CA that it is a currently-operating legal entity, along with several other attributes. EV certificates provide the highest level of assurance currently available. TLS clients (e.g., web browsers) consider EV certificates to be more trustworthy than certificates issued under other policies. Most web browsers display visual indicators a user is viewing a website secured with an EV certificate. Visual indicators provide additional assurance to the user that website they are viewing belongs to the company they intended to visit.

### Recommendation

EV certificates should be strongly considered by organizations if their users are likely to be targeted by phishing attacks. Phishing attacks often use typosquatted domain names (e.g., example.com versus example.com). Users of legitimate sites, who are accustomed to the visual indicators associated with EV certificates are more likely to notice such attacks.

### 2 findings

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
google.nyu.edu	COMODO CA Limited	216.165.84.74	443	3/6/2020, 5:33:03 AM
google.nyu.edu	COMODO CA Limited	128.122.109.58	443	3/6/2020, 3:09:33 AM

## !!! SSH Software Supports Vulnerable Protocol

-0.6 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.

### 11 findings

IP ADDRESS	PORT	LAST OBSERVED
128.122.130.1	22	3/4/2020, 6:21:45 PM
Evidence : protocol 1.99		
128.238.14.4	22	3/4/2020, 5:55:41 PM
Evidence : protocol 1.99		
128.122.195.7	22	3/4/2020, 4:05:33 PM
Evidence : protocol 1.99		
128.122.128.10	22	3/4/2020, 12:43:05 PM
Evidence : protocol 1.99		
128.122.195.17	22	3/4/2020, 11:54:13 AM
Evidence : protocol 1.99		
128.238.75.1	22	3/4/2020, 8:03:45 AM
Evidence : protocol 1.99		
216.165.101.2	22	3/4/2020, 7:42:51 AM
Evidence : protocol 1.99		
128.122.195.16	22	3/4/2020, 6:43:23 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : protocol 1.99		
128.238.28.41	22	3/4/2020, 4:09:31 AM
Evidence : protocol 1.99		
128.122.113.10	22	2/5/2020, 10:19:53 AM
Evidence : protocol 1.99		
128.122.130.89	22	2/4/2020, 8:23:54 PM
Evidence : protocol 1.99		

## !!! MongoDB Service Observed

-0.5 SCORE IMPACT

We observed MongoDB, a database management system, publicly exposed.

### Description

MongoDB is an open-source database management system (DBMS). DBMSes are intended to store large amounts of information. We observed a MongoDB service on the Internet, accessible by the public. DBMSes are attractive targets to attackers due to the data they may contain. An attacker that breaches a DBMS may sell the databases within, use them for blackmail, or employ the information when launching further attacks. A breached database 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 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.

### 2 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
MongoDB 4.2.0	128.122.136.124	27017	2/23/2020, 2:20:57 PM
MongoDB 3.2.4	216.165.117.136	27017	2/23/2020, 2:11:46 PM

## !! Certificate Is Expired

-0.6 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 the certificate a TLS server (e.g., website) presents to a client

### 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, while ensuring the clients that use

(e.g., web browser) is outside of those two dates, the client will refuse to connect to the server. Certificates are digital assets that require renewal or decommissioning on a schedule.

the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored. Evaluate the organization's certificate management policy to ensure that certificates are renewed or decommissioned prior to their expiration date.

## 53 findings

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	START DATE	EXPIRATION DATE	COLLECTION TARGET	PORT	LAST OBSERVED
jssanimosx.filmtv.ts oa.nyu.edu		1/23/2019, 10:35:10 PM	1/24/2020, 10:35:10 PM	128.122.100.101	8443	3/11/2020, 2:13:18 AM
its0115-elap-v.cfs.its.nyu.edu	Internet2	6/16/2016, 12:00:00 AM	6/16/2019, 11:59:59 PM	128.122.194.189	8443	3/10/2020, 11:38:16 PM
spark.stern.nyu.edu	Internet2	12/15/2014, 12:00:00 AM	12/14/2017, 11:59:59 PM	107.22.255.58	443	3/10/2020, 10:05:28 PM
hyper.ifa.nyu.edu	Internet2	10/2/2013, 12:00:00 AM	10/2/2015, 11:59:59 PM	128.122.65.146	8443	3/10/2020, 3:25:20 PM
nomad.noc.nyu.edu	Internet2	12/16/2014, 12:00:00 AM	12/15/2017, 11:59:59 PM	128.122.253.9	995	3/10/2020, 3:18:47 AM
nomad.noc.nyu.edu	Internet2	12/16/2014, 12:00:00 AM	12/15/2017, 11:59:59 PM	128.122.253.9	993	3/9/2020, 6:05:01 PM
hyper.ifa.nyu.edu	Internet2	10/2/2013, 12:00:00 AM	10/2/2015, 11:59:59 PM	128.122.65.146	636	3/9/2020, 3:42:57 AM
nomad.noc.nyu.edu	Internet2	12/16/2014, 12:00:00 AM	12/15/2017, 11:59:59 PM	128.122.253.9	465	3/8/2020, 8:51:31 AM
applicant-stg.stern.nyu.edu	Internet2	3/3/2016, 12:00:00 AM	3/3/2019, 11:59:59 PM	128.122.130.9	443	3/8/2020, 2:47:55 AM
execed-proxy.stern.nyu.edu	New York University	9/14/2017, 3:50:00 PM	9/14/2018, 3:50:00 PM	128.122.130.23	443	3/8/2020, 2:45:25 AM
datafacility.cusp.ny.edu	Internet2	12/13/2016, 12:00:00 AM	12/13/2019, 11:59:59 PM	128.122.72.213	443	3/7/2020, 6:14:36 PM
its0115-elap-v.cfs.its.nyu.edu	Internet2	6/16/2016, 12:00:00 AM	6/16/2019, 11:59:59 PM	128.122.194.189	443	3/7/2020, 10:25:01 AM
video.cims.nyu.edu	Internet2	1/19/2016, 12:00:00 AM	1/18/2019, 11:59:59 PM	128.122.49.114	443	3/7/2020, 8:38:49 AM
deploy.nursing.nyu.edu	Internet2	11/11/2015, 12:00:00 AM	11/10/2018, 11:59:59 PM	35.162.144.185	443	3/7/2020, 3:31:46 AM
shanghai.nyu.edu	Internet2	5/6/2016, 12:00:00 AM	5/6/2017, 11:59:59 PM	52.196.122.61	443	3/7/2020, 1:00:05 AM

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	START DATE	EXPIRATION DATE	COLLECTION TARGET	PORT	LAST OBSERVED
cauchy.cns.nyu.edu	New York University	11/19/2014, 12:45:09 AM	11/18/2017, 12:45:09 AM	128.122.112.30	443	3/7/2020, 12:40:58 AM
doc.bio.nyu.edu	Internet2	5/29/2012, 12:00:00 AM	5/29/2015, 11:59:59 PM	128.122.4.25	443	3/7/2020, 12:26:09 AM
aclmanager.nyu.edu	Internet2	2/10/2015, 12:00:00 AM	2/9/2018, 11:59:59 PM	128.122.128.72	443	3/7/2020, 12:14:50 AM
netmon.noc.nyu.edu	Internet2	1/28/2015, 12:00:00 AM	1/27/2018, 11:59:59 PM	128.122.128.45	443	3/6/2020, 11:56:01 PM
engineering.nyu.edu	SomeOrganization	4/27/2015, 3:17:12 PM	4/26/2016, 3:17:12 PM	52.5.55.254	443	3/6/2020, 11:54:45 PM
cue2.engineering.nyu.edu		8/7/2015, 7:56:11 PM	8/7/2016, 8:16:11 PM	216.165.117.5	443	3/6/2020, 10:47:01 PM
aquila.bio.nyu.edu	New York University	3/3/2010, 11:10:43 PM	4/2/2010, 11:10:43 PM	128.122.4.26	443	3/6/2020, 9:46:54 PM
request.bio.nyu.edu	Internet2	4/17/2015, 12:00:00 AM	4/16/2018, 11:59:59 PM	128.122.4.45	443	3/6/2020, 9:39:39 PM
vprnrasa-vl415-active.net.nyu.edu	Internet2	8/29/2016, 12:00:00 AM	9/11/2019, 11:59:59 PM	128.122.252.68	443	3/6/2020, 9:18:30 PM
mc.dlib.nyu.edu	SomeOrganization	4/24/2018, 4:36:50 PM	4/24/2019, 4:36:50 PM	128.122.108.91	443	3/6/2020, 6:25:32 PM
www.bookstores.ny.edu	Internet2	1/11/2016, 12:00:00 AM	4/8/2019, 11:59:59 PM	128.122.37.206	443	3/6/2020, 5:29:21 PM
www.bookstores.ny.edu	Internet2	1/11/2016, 12:00:00 AM	4/8/2019, 11:59:59 PM	128.122.37.209	443	3/6/2020, 5:08:56 PM
netmon.noc.nyu.edu	Internet2	1/28/2015, 12:00:00 AM	1/27/2018, 11:59:59 PM	128.122.128.23	443	3/6/2020, 11:39:48 AM
mobileprint.nyu.edu	Internet2	1/12/2016, 12:00:00 AM	1/11/2018, 11:59:59 PM	216.165.78.10	443	3/6/2020, 4:27:36 AM
newclasses.nyu.edu	Internet2	4/10/2015, 12:00:00 AM	4/9/2018, 11:59:59 PM	216.165.86.168	443	3/6/2020, 3:38:29 AM
hyper.ifa.nyu.edu	Internet2	10/2/2013, 12:00:00 AM	10/2/2015, 11:59:59 PM	128.122.65.146	443	3/6/2020, 1:29:31 AM
*.adlezp.med.nyu.edu	Internet2	2/9/2012, 12:00:00 AM	2/8/2015, 11:59:59 PM	216.165.125.225	443	3/5/2020, 11:12:28 PM
horatio.cs.nyu.edu	SomeOrganization	12/6/2018, 2:41:54 PM	12/6/2019, 2:41:54 PM	216.165.22.17	443	3/5/2020, 7:40:57 PM

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	START DATE	EXPIRATION DATE	COLLECTION TARGET	PORT	LAST OBSERVED
ais-stg.stern.nyu.edu	Internet2	11/3/2017, 12:00:00 AM	11/3/2018, 11:59:59 PM	128.122.130.150	443	3/5/2020, 4:51:29 PM
sso-d-sdc.stern.nyu.edu	Internet2	4/18/2016, 12:00:00 AM	4/18/2019, 11:59:59 PM	128.122.130.164	443	3/5/2020, 4:51:15 PM
vpnrasa-vl415-active.net.nyu.edu	Internet2	8/29/2016, 12:00:00 AM	9/11/2019, 11:59:59 PM	128.122.252.69	443	3/5/2020, 2:37:34 PM
vpn.nyu.edu	Internet2	8/29/2016, 12:00:00 AM	9/2/2019, 11:59:59 PM	128.122.252.77	443	3/5/2020, 2:21:40 PM
engineering.nyu.edu	SomeOrganization	4/27/2015, 3:17:12 PM	4/26/2016, 3:17:12 PM	52.4.249.152	443	3/5/2020, 9:27:19 AM
engineering.nyu.edu	Internet2	10/26/2017, 12:00:00 AM	11/8/2018, 11:59:59 PM	54.209.255.182	443	3/4/2020, 9:53:40 PM
iiq.nyu.edu	Internet2	1/14/2016, 12:00:00 AM	1/13/2019, 11:59:59 PM	216.165.85.206	443	3/4/2020, 9:35:42 PM
newhome.nyu.edu	Internet2	9/8/2015, 12:00:00 AM	9/7/2018, 11:59:59 PM	216.165.85.220	443	3/4/2020, 8:34:16 PM
ccs3usr.engineering.nyu.edu	Let's Encrypt	3/3/2019, 7:37:05 AM	6/1/2019, 7:37:05 AM	216.165.2.135	443	3/4/2020, 8:24:40 PM
nomad.noc.nyu.edu	Internet2	12/16/2014, 12:00:00 AM	12/15/2017, 11:59:59 PM	128.122.253.9	143	3/4/2020, 4:47:15 AM
nomad.noc.nyu.edu	Internet2	12/16/2014, 12:00:00 AM	12/15/2017, 11:59:59 PM	128.122.253.9	110	3/3/2020, 2:25:58 PM
courant.nyu.edu	Internet2	10/21/2016, 12:00:00 AM	10/21/2019, 11:59:59 PM	128.122.49.48	443	2/8/2020, 6:45:42 AM
symmetry.cs.nyu.edu	Internet2	1/15/2016, 12:00:00 AM	1/14/2019, 11:59:59 PM	128.122.49.59	443	2/8/2020, 6:29:41 AM
porta.law.nyu.edu	s Encrypt	3/19/2019, 1:21:07 AM	6/17/2019, 1:21:07 AM	128.122.94.94	443	2/8/2020, 2:32:31 AM
vpnsec.nyu.edu	Internet2	3/29/2016, 12:00:00 AM	3/29/2019, 11:59:59 PM	128.122.252.71	443	2/8/2020, 1:58:06 AM
spark.stern.nyu.edu	Internet2	12/15/2014, 12:00:00 AM	12/14/2017, 11:59:59 PM	23.23.104.134	443	2/7/2020, 7:17:51 PM
tick.nyu.edu	New York University	7/20/2009, 3:16:52 PM	7/19/2012, 3:16:52 PM	128.122.253.8	443	2/7/2020, 5:41:57 PM
nyu.edu	Internet2	1/29/2013, 12:00:00 AM	1/29/2016, 11:59:59 PM	216.165.85.207	443	2/6/2020, 2:10:14 PM

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	START DATE	EXPIRATION DATE	COLLECTION TARGET	PORT	LAST OBSERVED
novacore.law.nyu.edu	Internet2	1/10/2017, 12:00:00 AM	6/13/2019, 11:59:59 PM	128.122.159.143	443	2/6/2020, 12:20:14 AM
ems-dev.stern.nyu.edu	Internet2	7/15/2015, 12:00:00 AM	7/14/2018, 11:59:59 PM	128.122.130.34	443	2/5/2020, 2:06:02 PM

## !! 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.

### 500 findings

IP ADDRESS	PORT	LAST OBSERVED
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : aes256-cbc		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : 3des-cbc		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : arcfour256		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : blowfish-cbc		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : cast128-cbc		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : arcfour		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : aes192-cbc		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : arcfour128		
70.32.92.51	22	2/12/2020, 3:57:30 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : rijndael-cbc@lysator.liu.se		
70.32.92.51	22	2/12/2020, 3:57:30 PM
Evidence : aes128-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : arcfour		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : aes256-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : rijndael-cbc@lysator.liu.se		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : arcfour128		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : cast128-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : blowfish-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : aes192-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : 3des-cbc		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : arcfour256		
18.182.196.220	22	2/12/2020, 3:53:08 PM
Evidence : aes128-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : aes192-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : arcfour		
128.238.7.158	22	2/12/2020, 3:49:03 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour128		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : aes128-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : cast128-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : arcfour256		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : 3des-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : blowfish-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : aes256-cbc		
128.238.7.158	22	2/12/2020, 3:49:03 PM
Evidence : rijndael-cbc@lysator.liu.se		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : aes128-cbc		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : aes256-cbc		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : aes192-cbc		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : 3des-cbc		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : cast128-cbc		
35.245.188.255	22	2/12/2020, 3:40:33 PM
Evidence : blowfish-cbc		
193.175.54.7	22	2/12/2020, 3:32:19 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : 3des-cbc		
193.175.54.7	22	2/12/2020, 3:32:19 PM
Evidence : aes256-cbc		
193.175.54.7	22	2/12/2020, 3:32:19 PM
Evidence : aes128-cbc		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : 3des-cbc		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : arcfour		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : blowfish-cbc		
212.219.93.12	22	2/12/2020, 3:26:05 PM
Evidence : aes128-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : blowfish-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : aes128-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : arcfour256		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : 3des-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : aes256-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : arcfour128		
128.238.63.26	22	2/12/2020, 3:19:06 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : arcfour		
128.238.63.26	22	2/12/2020, 3:19:06 PM
Evidence : cast128-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : blowfish-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : 3des-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : aes192-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : arcfour128		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : aes128-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : arcfour		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : cast128-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : aes256-cbc		
128.238.66.31	22	2/12/2020, 3:04:34 PM
Evidence : arcfour256		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.149.48	22	2/12/2020, 3:01:44 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : 3des-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : blowfish-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : aes128-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : aes192-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : aes256-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : cast128-cbc		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : arcfour128		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : arcfour		
128.238.149.48	22	2/12/2020, 3:01:44 PM
Evidence : arcfour256		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : cast128-cbc		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : arcfour256		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : arcfour		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : 3des-cbc		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.182.20	22	2/12/2020, 3:00:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour128		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : aes256-cbc		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : aes192-cbc		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : aes128-cbc		
128.238.182.20	22	2/12/2020, 3:00:34 PM
Evidence : blowfish-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : arcfour256		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : 3des-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : arcfour128		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : aes256-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : arcfour		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : aes128-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : cast128-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : blowfish-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM
Evidence : aes192-cbc		
128.238.147.223	22	2/12/2020, 2:59:25 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : rijndael-cbc@lysator.liu.se		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : aes128-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : twofish128-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : aes192-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : twofish-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : twofish256-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : arcfour		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : blowfish-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : 3des-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : cast128-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : twofish192-cbc		
128.238.32.77	22	2/12/2020, 2:57:57 PM
Evidence : aes256-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : blowfish-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : arcfour256		
128.238.147.222	22	2/12/2020, 2:55:06 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour128		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : 3des-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : cast128-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : arcfour		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : aes128-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : aes256-cbc		
128.238.147.222	22	2/12/2020, 2:55:06 PM
Evidence : aes192-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : blowfish-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : aes128-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : aes192-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : 3des-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : aes256-cbc		
66.228.45.202	22	2/12/2020, 2:54:41 PM
Evidence : cast128-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : arcfour256		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : 3des-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : aes128-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : aes192-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : aes256-cbc		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : rijndael-cbc@lysator.liu.se		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : arcfour128		
34.231.198.186	22	2/12/2020, 2:50:28 PM
Evidence : blowfish-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : arcfour128		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : cast128-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : arcfour256		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : aes128-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : 3des-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : blowfish-cbc		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : arcfour		
128.238.66.5	22	2/12/2020, 2:44:56 PM
Evidence : aes256-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : aes256-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : cast128-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : aes128-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : blowfish-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : arcfour128		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : rijndael-cbc@lysator.liu.se		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : aes192-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : 3des-cbc		
35.155.171.240	22	2/12/2020, 2:39:34 PM
Evidence : arcfour256		
195.113.94.149	22	2/12/2020, 2:39:28 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes128-cbc		
195.113.94.149	22	2/12/2020, 2:39:28 PM
Evidence : 3des-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : 3des-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : aes256-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : blowfish-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : cast128-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : aes128-cbc		
159.65.160.172	22	2/12/2020, 2:32:57 PM
Evidence : aes192-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : arcfour256		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : rijndael-cbc@lysator.liu.se		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : arcfour		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : aes128-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : cast128-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : aes256-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour128		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : aes192-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : blowfish-cbc		
193.175.54.162	22	2/12/2020, 2:24:39 PM
Evidence : 3des-cbc		
128.238.62.69	22	2/12/2020, 2:24:12 PM
Evidence : aes128-cbc		
128.238.62.69	22	2/12/2020, 2:24:12 PM
Evidence : aes256-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : aes256-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : aes192-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : arcfour128		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : aes128-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : blowfish-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : cast128-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : arcfour		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : 3des-cbc		
128.238.24.232	22	2/12/2020, 2:20:36 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : rijndael-cbc@lysator.liu.se		
128.238.24.232	22	2/12/2020, 2:20:36 PM
Evidence : arcfour256		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : arcfour128		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : arcfour		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : aes256-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : aes192-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : cast128-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : aes128-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : blowfish-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : 3des-cbc		
128.238.182.100	22	2/12/2020, 2:18:37 PM
Evidence : arcfour256		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : arcfour		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : arcfour128		
128.238.147.215	22	2/12/2020, 2:16:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : blowfish-cbc		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : 3des-cbc		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : arcfour256		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : aes128-cbc		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : cast128-cbc		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : aes256-cbc		
128.238.147.215	22	2/12/2020, 2:16:00 PM
Evidence : aes192-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : 3des-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : rijndael-cbc@lysator.liu.se		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : cast128-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : arcfour128		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : aes256-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : arcfour		
107.180.61.237	22	2/12/2020, 2:12:57 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour256		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : aes128-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : blowfish-cbc		
107.180.61.237	22	2/12/2020, 2:12:57 PM
Evidence : aes192-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : arcfour		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : aes192-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : rijndael-cbc@lysator.liu.se		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : arcfour128		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : blowfish-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : aes128-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : 3des-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : aes256-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : cast128-cbc		
13.231.227.172	22	2/12/2020, 2:12:10 PM
Evidence : arcfour256		
128.238.147.208	22	2/12/2020, 2:07:03 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes256-cbc		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : arcfour256		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : aes128-cbc		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : arcfour		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : aes192-cbc		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : arcfour128		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : blowfish-cbc		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : cast128-cbc		
128.238.147.208	22	2/12/2020, 2:07:03 PM
Evidence : 3des-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM
Evidence : blowfish-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM
Evidence : aes128-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM
Evidence : aes256-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM
Evidence : aes192-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : 3des-cbc		
128.238.147.24	22	2/12/2020, 1:55:11 PM
Evidence : cast128-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : arcfour128		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : aes192-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : cast128-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : aes128-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : rijndael-cbc@lysator.liu.se		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : arcfour256		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : 3des-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : blowfish-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : aes256-cbc		
195.113.94.147	22	2/12/2020, 1:48:19 PM
Evidence : arcfour		
70.32.96.242	22	2/12/2020, 1:47:59 PM
Evidence : 3des-cbc		
70.32.96.242	22	2/12/2020, 1:47:59 PM
Evidence : aes256-cbc		
70.32.96.242	22	2/12/2020, 1:47:59 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
70.32.96.242	22	2/12/2020, 1:47:59 PM
Evidence : blowfish-cbc		
70.32.96.242	22	2/12/2020, 1:47:59 PM
Evidence : aes128-cbc		
70.32.96.242	22	2/12/2020, 1:47:59 PM
Evidence : cast128-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : aes128-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : arcfour128		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : 3des-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : blowfish-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : arcfour		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : aes256-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : rijndael-cbc@lysator.liu.se		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : arcfour256		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : cast128-cbc		
52.1.126.186	22	2/12/2020, 1:44:26 PM
Evidence : aes192-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM
Evidence : aes256-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM
Evidence : 3des-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM
Evidence : blowfish-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM
Evidence : cast128-cbc		
3.20.35.173	22	2/12/2020, 1:41:04 PM
Evidence : aes128-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : blowfish-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : arcfour256		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : arcfour128		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : aes192-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : cast128-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : arcfour		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : aes128-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes256-cbc		
128.238.38.77	22	2/12/2020, 1:34:58 PM
Evidence : 3des-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : cast128-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : blowfish-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : 3des-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : aes192-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : aes128-cbc		
18.178.238.184	22	2/12/2020, 1:32:32 PM
Evidence : aes256-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : aes256-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : arcfour128		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : arcfour256		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : blowfish-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : aes128-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : aes192-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : 3des-cbc		
128.238.66.173	22	2/12/2020, 1:23:25 PM
Evidence : arcfour		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : cast128-cbc		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : rijndael-cbc@lysator.liu.se		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : blowfish-cbc		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : arcfour		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : arcfour256		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : 3des-cbc		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : aes256-cbc		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : arcfour128		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : aes192-cbc		
216.165.2.19	22	2/12/2020, 1:22:23 PM
Evidence : aes128-cbc		
212.219.93.7	22	2/12/2020, 1:19:48 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes128-cbc		
212.219.93.7	22	2/12/2020, 1:19:48 PM
Evidence : aes256-cbc		
212.219.93.7	22	2/12/2020, 1:19:48 PM
Evidence : 3des-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : blowfish-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : 3des-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : cast128-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : aes256-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : arcfour256		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : aes192-cbc		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : arcfour		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : arcfour128		
128.238.147.216	22	2/12/2020, 1:13:30 PM
Evidence : aes128-cbc		
128.238.118.20	22	2/12/2020, 1:11:45 PM
Evidence : aes256-cbc		
128.238.118.20	22	2/12/2020, 1:11:45 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : 3des-cbc		
128.238.118.20	22	2/12/2020, 1:11:45 PM
Evidence : aes128-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : aes128-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : 3des-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : cast128-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : aes256-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : blowfish-cbc		
3.216.211.57	22	2/12/2020, 1:04:45 PM
Evidence : aes192-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : blowfish-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : aes192-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : arcfour128		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : aes128-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : arcfour256		
128.238.147.230	22	2/12/2020, 1:00:53 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes256-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : 3des-cbc		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : arcfour		
128.238.147.230	22	2/12/2020, 1:00:53 PM
Evidence : cast128-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : cast128-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : aes192-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : aes256-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : 3des-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : aes128-cbc		
18.182.244.218	22	2/12/2020, 12:55:51 PM
Evidence : blowfish-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : arcfour256		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : arcfour		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : cast128-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : arcfour128		
128.238.182.5	22	2/12/2020, 12:52:48 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : rijndael-cbc@lysator.liu.se		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : blowfish-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : aes128-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : aes256-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : 3des-cbc		
128.238.182.5	22	2/12/2020, 12:52:48 PM
Evidence : aes192-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : arcfour128		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : 3des-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : aes256-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : cast128-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : blowfish-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : arcfour		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : aes128-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
128.238.7.156	22	2/12/2020, 12:50:33 PM
Evidence : arcfour256		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : aes128-cbc		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : aes192-cbc		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : aes256-cbc		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : arcfour256		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : arcfour128		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : 3des-cbc		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : blowfish-cbc		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : arcfour		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.182.10	22	2/12/2020, 12:33:39 PM
Evidence : cast128-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : aes128-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : cast128-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : arcfour128		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : arcfour		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : aes192-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : aes256-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : blowfish-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : 3des-cbc		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : arcfour256		
34.193.12.206	22	2/12/2020, 12:31:00 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.75.1	22	2/12/2020, 12:30:35 PM
Evidence : 3des-cbc		
128.238.75.1	22	2/12/2020, 12:30:35 PM
Evidence : aes256-cbc		
128.238.75.1	22	2/12/2020, 12:30:35 PM
Evidence : aes128-cbc		
128.238.75.1	22	2/12/2020, 12:30:35 PM
Evidence : aes192-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM
Evidence : blowfish-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM
Evidence : 3des-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes128-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM
Evidence : cast128-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM
Evidence : aes256-cbc		
128.238.26.21	22	2/12/2020, 12:30:18 PM
Evidence : aes192-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : cast128-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : 3des-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : aes192-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : blowfish-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : aes128-cbc		
18.182.119.242	22	2/12/2020, 12:28:55 PM
Evidence : aes256-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : arcfour256		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : arcfour128		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : aes256-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : aes128-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : blowfish-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : arcfour		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : rijndael-cbc@lysator.liu.se		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : 3des-cbc		
195.113.94.20	22	2/12/2020, 12:27:39 PM
Evidence : aes192-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : aes256-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : aes192-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : arcfour		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : rijndael-cbc@lysator.liu.se		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : blowfish-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : 3des-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : arcfour256		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : arcfour128		
52.0.197.6	22	2/12/2020, 12:23:53 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
52.0.197.6	22	2/12/2020, 12:23:53 PM
Evidence : aes128-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : cast128-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : 3des-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : arcfour256		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : arcfour		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : aes256-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : aes192-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : blowfish-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : aes128-cbc		
128.238.66.35	22	2/12/2020, 12:08:10 PM
Evidence : arcfour128		
35.172.243.166	22	2/12/2020, 12:07:40 PM
Evidence : 3des-cbc		
35.172.243.166	22	2/12/2020, 12:07:40 PM
Evidence : aes256-cbc		
35.172.243.166	22	2/12/2020, 12:07:40 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes192-cbc		
35.172.243.166	22	2/12/2020, 12:07:40 PM
Evidence : blowfish-cbc		
35.172.243.166	22	2/12/2020, 12:07:40 PM
Evidence : aes128-cbc		
35.172.243.166	22	2/12/2020, 12:07:40 PM
Evidence : cast128-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : aes192-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : aes128-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : cast128-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : aes256-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : blowfish-cbc		
128.238.26.49	22	2/12/2020, 12:05:08 PM
Evidence : 3des-cbc		
13.114.219.73	22	2/12/2020, 11:54:28 AM
Evidence : aes128-cbc		
13.114.219.73	22	2/12/2020, 11:54:28 AM
Evidence : blowfish-cbc		
13.114.219.73	22	2/12/2020, 11:54:28 AM
Evidence : cast128-cbc		
13.114.219.73	22	2/12/2020, 11:54:28 AM
Evidence : 3des-cbc		
13.114.219.73	22	2/12/2020, 11:54:28 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes256-cbc		
13114.219.73	22	2/12/2020, 11:54:28 AM
Evidence : aes192-cbc		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : aes128-cbc		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : aes192-cbc		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : aes256-cbc		
128.238.14.4	22	2/12/2020, 11:54:09 AM
Evidence : 3des-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : rijndael-cbc@lysator.liu.se		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : aes128-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : 3des-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : arcfour128		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : cast128-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : aes192-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : arcfour		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : aes256-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : blowfish-cbc		
45.55.130.164	22	2/12/2020, 11:48:33 AM
Evidence : arcfour256		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : 3des-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : aes128-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : aes192-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : arcfour		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : arcfour256		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : blowfish-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : cast128-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : aes256-cbc		
128.238.66.55	22	2/12/2020, 11:46:59 AM
Evidence : arcfour128		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : blowfish-cbc		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : aes192-cbc		
193.175.54.5	22	2/12/2020, 11:46:37 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : aes256-cbc		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : aes128-cbc		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : arcfour		
193.175.54.5	22	2/12/2020, 11:46:37 AM
Evidence : 3des-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : arcfour		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : aes192-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : aes128-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : arcfour256		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : aes256-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : 3des-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : blowfish-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : cast128-cbc		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : rijndael-cbc@lysator.liu.se		
192.86.139.64	22	2/12/2020, 11:43:58 AM
Evidence : arcfour128		
128.238.182.102	22	2/12/2020, 11:41:50 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
128.238.182.102	22	2/12/2020, 11:41:50 AM
Evidence : 3des-cbc		
128.238.182.102	22	2/12/2020, 11:41:50 AM
Evidence : blowfish-cbc		
128.238.182.102	22	2/12/2020, 11:41:50 AM
Evidence : aes256-cbc		
128.238.182.102	22	2/12/2020, 11:41:50 AM
Evidence : aes192-cbc		
128.238.182.102	22	2/12/2020, 11:41:50 AM
Evidence : aes128-cbc		
192.76.177.149	22	2/12/2020, 11:37:08 AM
Evidence : aes256-cbc		
192.76.177.149	22	2/12/2020, 11:37:08 AM
Evidence : aes128-cbc		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : aes256-cbc		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : arcfour128		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : blowfish-cbc		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : aes192-cbc		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : arcfour256		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : rijndael-cbc@lysator.liu.se		
128.238.182.21	22	2/12/2020, 11:34:55 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

IP ADDRESS	PORT	LAST OBSERVED
Evidence : cast128-cbc		
128.238.182.21	22	2/12/2020, 11:34:55 AM
Evidence : 3des-cbc		

## !! IMAP Service Observed

-0.3 SCORE IMPACT

We observed IMAP, an email retrieval service, publicly exposed.

### Description

The IMAP protocol offers access to messages stored on email servers. IMAP servers frequently contain all messages ever sent or received by an email account, not just recent messages. We observed an IMAP service on the Internet, accessible by the public. Email retrieval services are attractive targets to attackers due to the data they may contain. An attacker that gains access to an email account's messages may use them for blackmail, impersonating the owner of the email account, or employ the information when launching further attacks. An attacker with access to an email account's messages may gain access to many online accounts associated with that email address by using the password reset functions available on most websites. 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 access the messages within. 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.

### Recommendation

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

## 27 findings

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Dovecot imapd	159.65.160.172	5000	3/9/2020, 4:18:31 PM
Dovecot imapd	37.60.232.214	143	3/9/2020, 2:11:18 AM
Dovecot imapd	128.122.205.35	143	3/9/2020, 2:05:30 AM
Dovecot imapd	128.122.49.90	143	3/9/2020, 1:01:03 AM
Dovecot imapd	128.122.49.91	143	3/9/2020, 12:59:11 AM
Dovecot imapd	107.180.61.237	143	3/9/2020, 12:40:40 AM
Courier Imapd	70.32.92.51	143	3/9/2020, 12:30:12 AM
Dovecot imapd	128.122.250.124	143	3/9/2020, 12:18:03 AM
Dovecot imapd	70.32.96.242	143	3/8/2020, 10:32:34 PM
Dovecot imapd	128.122.87.78	143	3/8/2020, 10:11:37 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

PRODUCT NAME	IP ADDRESS	PORT	LAST OBSERVED
Dovecot imapd	128.122.253.9	143	3/8/2020, 9:11:22 PM
Dovecot imapd	35.214.191.115	143	3/8/2020, 8:56:50 PM
Novell GroupWise imapd	128.122.158.3	143	3/8/2020, 8:20:58 PM
Courier Imapd	128.122.161.15	143	3/8/2020, 8:13:57 PM
Dovecot imapd	159.65.160.172	139	3/7/2020, 11:01:13 PM
Dovecot imapd	159.65.160.172	1434	3/3/2020, 12:12:05 PM
Dovecot imapd	159.65.160.172	3389	2/26/2020, 4:09:41 PM
Dovecot imapd	128.122.87.78	993	2/14/2020, 9:58:48 AM
Dovecot imapd	128.122.49.90	993	2/14/2020, 9:19:22 AM
Dovecot imapd	128.122.205.35	993	2/14/2020, 8:40:03 AM
Dovecot imapd	35.214.191.115	993	2/14/2020, 8:25:54 AM
Dovecot imapd	70.32.96.242	993	2/14/2020, 7:57:58 AM
Dovecot imapd	128.122.253.9	993	2/14/2020, 7:52:29 AM
Courier Imapd	70.32.92.51	993	2/14/2020, 5:37:35 AM
Dovecot imapd	107.180.61.237	993	2/14/2020, 5:04:51 AM
Courier Imapd	128.122.161.15	993	2/14/2020, 5:03:04 AM
Dovecot imapd	128.122.49.91	993	2/14/2020, 4:55:22 AM

## !! Certificate Is Self-Signed

-0.3 SCORE IMPACT

Servers presenting self-signed certificates trigger warnings in, or prevent connections from TLS clients.

### Description

When a certificate is issued, it is 'signed' by a certificate authority (CA). Signatures are attestations of the certificate-holder's identity. TLS clients (e.g., web browsers) maintain trust stores, which are lists of CAs whose attestations they trust. The ability to sign a certificate may be delegated from a CA to another entity, such as a subsidiary, creating chains of attestations. In the context of chains of attestation, the delegating CA is the root CA, and the delegated CA is the intermediate CA. Trust stores in TLS clients may contain both intermediate and root CAs. TLS clients validate a server's certificate by tracing its chain of attestations back to a CA in its trust store. Certificates that are self-signed have no chain of attestations: they are self-attested. This means that most TLS clients, when presented with a self-signed certificate, will display a warning before connecting to the server, or refuse to connect to the server. Off-the-shelf software and hardware

### Recommendation

Services presenting self-signed certificates should cause noticeable failures or user-visible warnings, so confirm the service is still in use. If the service is not in use, decommission it. Otherwise, contact your CA and arrange issuance of a new certificate, while ensuring the clients that use the service are configured to validate certificates when making TLS connections. If the clients were configured to validate certificates, ensure that their errors are monitored.

frequently runs services that use self-signed certificates by default. Many of these services can be configured to use certificates that are not self-signed. The use of self-signed certificates may result in TLS clients being configured to skip validating certificates, making their connections vulnerable to man-in-the-middle attacks. Users that bypass their web browser's warning upon connecting to a server presenting a self-signed certificate are also vulnerable to man-in-the-middle attacks. Self-signed certificates have narrow, but legitimate use cases, such as protecting services whose clients are configured to use public key pinning.

#### 4 findings

CERTIFICATE COMMON NAME	CERTIFICATE AUTHORITY	COLLECTION TARGET	PORT	LAST OBSERVED
*.leoyan.com	Leoyan	216.165.22.6	443	3/7/2020, 1:21:51 AM
ftyjss_serverosx.filmtv.tsoa.ny.edu		128.122.102.203	443	3/6/2020, 11:44:00 PM
cue2.engineering.nyu.edu		216.165.117.5	443	3/6/2020, 10:47:01 PM
cue1.engineering.nyu.edu		216.165.116.103	443	3/6/2020, 10:18:49 AM

 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

**i INFORMATIONAL**

There are no Informational Signals for Hacker Chatter

No issues found

## C 70 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 High Severity CVEs Patching Cadence	End-of-Service Product Medium Severity CVEs Patching Cadence End-of-Life Product Medium-Severity Vulnerability in Last Observation	1 881 1 1,525	24 6
INFORMATIONAL			
			There are no Positive Signals for Patching Cadence
			There are no Informational Signals for Patching Cadence

### !! End-of-Service Product

-0.1 SCORE IMPACT

We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.

#### Description

A product that has been declared as end-of-service (EOS) by the manufacturer has been detected. An EOS product is no longer eligible for any support, security patches, or replacement parts. Products at this stage in their life cycle are more likely to have vulnerabilities that need to be patched, but without service support those vulnerabilities will persist until the product is replaced. Using EOS products also violates several compliance frameworks, including PCI DSS and HIPAA.

#### Recommendation

Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.

1 finding

PRODUCT VERSION	IP ADDRESS	PORT	END OF LIFE DATE	PRODUCT MANUFACTURER	PRODUCT NAME	MANUFACTURER STATEMENT	LAST OBSERVED
6.0	128.122.65.243	80	7/14/2015, 12:00:00 AM	Microsoft	Internet Information Services 6.0	<a href="https://support.microsoft.com/en-us/lifecycle?p1=2097">https://support.microsoft.com/en-us/lifecycle?p1=2097</a>	3/7/2020, 5:59:06 AM

### !! Medium Severity CVEs Patching Cadence

-0.7 SCORE IMPACT

Medium severity vulnerability seen on network more than 60 days after CVE was published.

#### Description

Based on scan data, the company had medium severity CVE vulnerability that was open longer than 60 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 practice to mitigate or patch medium severity vulnerabilities within 60 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 BugTraq mailing list 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.

## 500 findings

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-0777	192.86.139.65	22	1/13/2020, 12:45:11 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-2016-0777	192.86.139.66	22	1/12/2020, 9:31:18 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-2015-3183	128.122.4.238	443	1/12/2020, 9:33:25 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	128.122.4.238	443	1/12/2020, 9:33:25 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.4.238	443	1/12/2020, 9:33:25 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-2015-3185	128.122.4.238	443	1/12/2020, 9:33:25 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-7529	34.193.12.206	443	1/12/2020, 9:02:31 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-2014-0226	128.122.120.72	443	1/12/2020, 1:56:40 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-0232	128.122.120.72	443	1/12/2020, 1:56:40 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-3670	128.122.120.72	443	1/12/2020, 1:56:40 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2017-3773	128.122.120.72	443	1/12/2020, 1:56:40 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-3597	128.122.120.72	443	1/12/2020, 1:56:40 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2016-8743	128.122.149.114	443	1/12/2020, 12:34:34 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-2016-8743	128.122.108.12	443	1/12/2020, 12:31:02 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-2016-0703	128.122.85.67	443	1/11/2020, 11:54:41 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-2015-3194	128.122.85.67	443	1/11/2020, 11:54:41 PM	12/6/2015, 12:00:00 AM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2015-3197	128.122.85.67	443	1/11/2020, 11:54:41 PM	2/14/2016, 12:00:00 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2015-3195	128.122.85.67	443	1/11/2020, 11:54:41 PM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2016-8743	128.122.130.116	443	1/11/2020, 11:35:35 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-2015-4021	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.				
CVE-2015-2783	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.				
CVE-2015-3330	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."				
CVE-2015-4024	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.				
CVE-2017-3738	52.1.187.2	443	1/11/2020, 6:38:58 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	52.1.187.2	443	1/11/2020, 6:38:58 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	52.1.187.2	443	1/11/2020, 6:38:58 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	52.1.187.2	443	1/11/2020, 6:38:58 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	52.1.187.2	443	1/11/2020, 6:38:58 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-2014-0226	52.1.187.2	443	1/11/2020, 6:38:58 PM	7/20/2014, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	52.1187.2	443	1/11/2020, 6:38:58 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3737	128.122.49.17	443	1/11/2020, 5:57:03 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	128.122.49.17	443	1/11/2020, 5:57:03 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.122.49.17	443	1/11/2020, 5:57:03 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-0232	128.122.49.17	443	1/11/2020, 5:57:03 PM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2016-8743	128.122.49.17	443	1/11/2020, 5:57:03 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-2015-3185	128.122.49.17	443	1/11/2020, 5:57:03 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.17	443	1/11/2020, 5:57:03 PM	7/20/2014, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3597	128.122.49.17	443	1/11/2020, 5:57:03 PM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2014-3670	128.122.49.17	443	1/11/2020, 5:57:03 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3738	128.122.49.17	443	1/11/2020, 5:57:03 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.122.49.123	443	1/11/2020, 5:56:49 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-2017-5647	216.165.48.14	443	1/11/2020, 5:39:19 PM	4/17/2017, 12:00:00 AM
Vulnerability Description : A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.				
CVE-2017-12617	216.165.48.14	443	1/11/2020, 5:39:19 PM	10/3/2017, 12:00:00 AM
Vulnerability Description : When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.				
CVE-2017-5664	216.165.48.14	443	1/11/2020, 5:39:19 PM	6/6/2017, 12:00:00 AM
Vulnerability Description : The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.				
CVE-2016-8743	216.165.113.171	443	1/11/2020, 5:28:33 PM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2016-8743	128.122.108.143	443	1/11/2020, 3:53:38 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-2016-0703	128.122.108.158	443	1/11/2020, 3:44:40 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-2015-3195	128.122.108.158	443	1/11/2020, 3:44:40 PM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2016-8743	128.122.108.158	443	1/11/2020, 3:44:40 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-2017-3737	128.238.63.88	443	1/11/2020, 3:43:47 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.238.63.88	443	1/11/2020, 3:43:47 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.238.63.88	443	1/11/2020, 3:43:47 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-2017-3738	128.238.63.88	443	1/11/2020, 3:43:47 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-0226	128.238.63.88	443	1/11/2020, 3:43:47 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.238.63.88	443	1/11/2020, 3:43:47 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.238.63.88	443	1/11/2020, 3:43:47 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.49.35	443	1/11/2020, 11:26:15 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	128.122.49.35	443	1/11/2020, 11:26:15 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.122.49.35	443	1/11/2020, 11:26:15 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.122.49.35	443	1/11/2020, 11:26:15 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-2017-3737	128.122.49.35	443	1/11/2020, 11:26:15 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3185	128.122.49.35	443	1/11/2020, 11:26:15 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.49.35	443	1/11/2020, 11:26:15 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.49.29	443	1/11/2020, 10:02:40 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.29	443	1/11/2020, 10:02:40 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	128.122.49.29	443	1/11/2020, 10:02:40 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.49.29	443	1/11/2020, 10:02:40 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-2017-3736	128.122.49.29	443	1/11/2020, 10:02:40 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	128.122.49.29	443	1/11/2020, 10:02:40 AM	7/20/2015, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.122.49.29	443	1/11/2020, 10:02:40 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	91.230.41.15	443	1/11/2020, 9:40:26 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-2015-3183	91.230.41.15	443	1/11/2020, 9:40:26 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	91.230.41.15	443	1/11/2020, 9:40:26 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	91.230.41.15	443	1/11/2020, 9:40:26 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.238.193	443	1/11/2020, 6:23:24 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-2016-8743	128.122.108.64	443	1/11/2020, 12:26:18 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-2016-8743	128.122.108.13	443	1/11/2020, 12:23:19 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-2016-8743	128.122.112.23	443	1/11/2020, 12:11:51 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-2016-0703	128.122.128.31	443	1/10/2020, 10:13:36 PM	3/2/2016, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2016-8743	128.122.128.31	443	1/10/2020, 10:13:36 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-2016-8743	128.122.108.23	443	1/10/2020, 6:06:58 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-2016-8743	128.122.163.137	443	1/10/2020, 5:36:38 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-2015-3185	128.122.163.137	443	1/10/2020, 5:36:38 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.163.137	443	1/10/2020, 5:36:38 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.163.137	443	1/10/2020, 5:36:38 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.163.137	443	1/10/2020, 5:36:38 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3737	128.122.163.137	443	1/10/2020, 5:36:38 PM	12/7/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2014-0226	128.122.163.137	443	1/10/2020, 5:36:38 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	128.122.94.100	80	1/8/2020, 2:07:35 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.94.100	80	1/8/2020, 2:07:35 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	128.122.94.100	80	1/8/2020, 2:07:35 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2016-8743	128.122.94.100	80	1/8/2020, 2:07:35 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-2017-3736	128.122.94.100	80	1/8/2020, 2:07:35 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.94.100	80	1/8/2020, 2:07:35 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.94.100	80	1/8/2020, 2:07:35 PM	12/7/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-0703	128.122.128.23	80	1/8/2020, 10:46:32 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-2016-8743	128.122.40.84	80	1/8/2020, 9:11:40 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-2016-8743	128.122.34.205	80	1/8/2020, 8:45:44 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-2017-3738	216.165.26.109	80	1/8/2020, 4:14:05 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	216.165.26.109	80	1/8/2020, 4:14:05 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-2014-0226	216.165.26.109	80	1/8/2020, 4:14:05 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	216.165.26.109	80	1/8/2020, 4:14:05 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-0232	216.165.26.109	80	1/8/2020, 4:14:05 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-3670	216.165.26.109	80	1/8/2020, 4:14:05 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3737	216.165.26.109	80	1/8/2020, 4:14:05 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	216.165.26.109	80	1/8/2020, 4:14:05 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	216.165.26.109	80	1/8/2020, 4:14:05 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-3597	216.165.26.109	80	1/8/2020, 4:14:05 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2014-3566	128.122.121.159	443	1/8/2020, 3:24:10 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.133.153	80	1/8/2020, 3:00:33 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-2016-8743	128.122.108.12	80	1/8/2020, 2:32:54 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-2015-3197	128.122.85.67	80	1/8/2020, 1:52:52 AM	2/14/2016, 12:00:00 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3195	128.122.85.67	80	1/8/2020, 1:52:52 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2015-3194	128.122.85.67	80	1/8/2020, 1:52:52 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2016-0703	128.122.85.67	80	1/8/2020, 1:52:52 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-2016-8743	128.122.130.19	80	1/8/2020, 1:28:13 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-2014-3566	216.165.83.77	443	1/7/2020, 8:22:52 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-4021	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.				
CVE-2015-2783	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.				
CVE-2015-3330	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."				
CVE-2015-4024	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.				
CVE-2017-7529	128.122.26.159	80	1/7/2020, 4:53:12 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-2016-8743	128.122.108.161	80	1/7/2020, 4:28:36 PM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2016-8743	128.122.130.52	80	1/7/2020, 1:30:43 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-2016-0703	128.122.128.34	80	1/7/2020, 1:13:12 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-2017-7529	128.122.85.97	80	1/7/2020, 12:51:21 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-2016-4450	128.122.85.97	80	1/7/2020, 12:51:21 PM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2014-3556	128.122.85.97	80	1/7/2020, 12:51:21 PM	12/29/2014, 12:00:00 AM
Vulnerability Description : The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.				
CVE-2016-8743	128.122.4.26	80	1/7/2020, 11:40:26 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-2015-3183	128.122.49.20	80	1/7/2020, 9:49:45 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	128.122.49.20	80	1/7/2020, 9:49:45 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	128.122.49.20	80	1/7/2020, 9:49:45 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read() / SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read() / SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2017-3736	128.122.49.20	80	1/7/2020, 9:49:45 AM	1/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.49.20	80	1/7/2020, 9:49:45 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-2014-3597	128.122.49.20	80	1/7/2020, 9:49:45 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-3185	128.122.49.20	80	1/7/2020, 9:49:45 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-0232	128.122.49.20	80	1/7/2020, 9:49:45 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3738	128.122.49.20	80	1/7/2020, 9:49:45 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-3670	128.122.49.20	80	1/7/2020, 9:49:45 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.122.238.193	80	1/7/2020, 5:40:07 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-2016-8743	128.122.34.211	80	1/7/2020, 3:44:34 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3185	128.122.34.211	80	1/7/2020, 3:44:34 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.34.211	80	1/7/2020, 3:44:34 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.34.211	80	1/7/2020, 3:44:34 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3566	128.122.108.158	443	1/7/2020, 2:21:10 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.238.63.88	443	1/7/2020, 2:17:11 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2017-3736	216.165.47.13	80	1/7/2020, 12:58:38 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	216.165.47.13	80	1/7/2020, 12:58:38 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	216.165.47.13	80	1/7/2020, 12:58:38 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	216.165.47.13	80	1/7/2020, 12:58:38 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-0226	216.165.47.13	80	1/7/2020, 12:58:38 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	216.165.47.13	80	1/7/2020, 12:58:38 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-10.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	216.165.47.13	80	1/7/2020, 12:58:38 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-2016-8743	128.122.230.148	80	1/7/2020, 12:48:30 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-2016-8743	128.122.230.132	80	1/7/2020, 12:48:09 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-2016-8743	128.122.230.149	80	1/7/2020, 12:39:57 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-2014-3566	199.119.125.133	443	1/6/2020, 7:23:25 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.149.174	80	1/6/2020, 4:40:33 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-2017-7529	128.122.167.48	80	1/6/2020, 4:30:18 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-2016-4450	128.122.167.48	80	1/6/2020, 4:30:18 PM	6/7/2016, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-8743	128.122.130.142	80	1/6/2020, 4:26:09 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-2014-3566	128.122.104.181	443	1/6/2020, 10:58:35 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-6170	128.238.32.22	53	1/6/2020, 9:20:54 AM	7/6/2016, 12:00:00 AM
Vulnerability Description : ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message.				
CVE-2015-8704	128.238.32.22	53	1/6/2020, 9:20:54 AM	1/20/2016, 12:00:00 AM
Vulnerability Description : apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.				
CVE-2016-9444	128.238.32.22	53	1/6/2020, 9:20:54 AM	1/12/2017, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.				
CVE-2016-1286	128.238.32.22	53	1/6/2020, 9:20:54 AM	3/9/2016, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.				
CVE-2015-8000	128.238.32.22	53	1/6/2020, 9:20:54 AM	12/16/2015, 12:00:00 AM
Vulnerability Description : db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.				
CVE-2016-8864	128.238.32.22	53	1/6/2020, 9:20:54 AM	1/12/2016, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.				
CVE-2016-1285	128.238.32.22	53	1/6/2020, 9:20:54 AM	3/9/2016, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c.				
CVE-2016-9131	128.238.32.22	53	1/6/2020, 9:20:54 AM	1/12/2017, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.				
CVE-2014-3566	128.122.238.193	443	1/6/2020, 7:37:39 AM	10/14/2014, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-0204	128.122.128.31	443	1/5/2020, 3:25:23 PM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-4000	128.122.128.31	443	1/5/2020, 3:25:23 PM	5/20/2015, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.				
CVE-2016-8743	91.230.41.53	80	1/5/2020, 10:49:24 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-2014-3566	216.165.117.135	443	1/5/2020, 5:11:56 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-0777	128.122.4.239	22	1/5/2020, 3:46:05 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-2016-0777	128.122.172.20	22	1/5/2020, 1:23:05 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-2016-0777	128.122.60.87	22	1/5/2020, 12:43:52 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-2016-0777	128.122.86.132	22	1/4/2020, 11:54:03 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-2016-0777	128.122.251.94	22	1/4/2020, 10:18:43 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-2016-0777	128.122.208.213	22	1/4/2020, 9:45:33 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-2016-0777	128.122.10.52	22	1/4/2020, 9:30:38 PM	1/14/2016, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2016-6210	128.122.141.21	22	1/4/2020, 7:11:36 PM	2/13/2017, 12:00:00 AM
Vulnerability Description : sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.				
CVE-2016-0777	128.122.167.33	22	1/4/2020, 12:56:34 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-2016-0777	128.122.167.74	22	1/4/2020, 12:35:36 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-2016-0777	128.122.86.19	22	1/4/2020, 12:30:13 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-2016-8743	216.165.2.60	8080	12/30/2019, 5:50:53 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-2015-0232	128.122.4.48	443	12/19/2019, 9:56:11 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3737	128.122.4.48	443	12/19/2019, 9:56:11 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-3597	128.122.4.48	443	12/19/2019, 9:56:11 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2017-3738	128.122.4.48	443	12/19/2019, 9:56:11 AM	12/7/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.4.48	443	12/19/2019, 9:56:11 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.4.48	443	12/19/2019, 9:56:11 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-2015-3185	128.122.4.48	443	12/19/2019, 9:56:11 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.4.48	443	12/19/2019, 9:56:11 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-0226	128.122.4.48	443	12/19/2019, 9:56:11 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3670	128.122.4.48	443	12/19/2019, 9:56:11 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.122.128.25	443	12/19/2019, 9:55:52 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-2016-0703	128.122.128.25	443	12/19/2019, 9:55:52 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-8743	128.122.130.68	443	12/19/2019, 8:50:55 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-2017-3736	128.122.94.100	443	12/19/2019, 8:30:24 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-0226	128.122.94.100	443	12/19/2019, 8:30:24 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	128.122.94.100	443	12/19/2019, 8:30:24 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.122.94.100	443	12/19/2019, 8:30:24 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.122.94.100	443	12/19/2019, 8:30:24 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.94.100	443	12/19/2019, 8:30:24 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-2017-3738	128.122.94.100	443	12/19/2019, 8:30:24 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-8743	128.122.130.19	443	12/19/2019, 8:15:45 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-2016-0703	128.238.66.31	443	12/19/2019, 5:29:34 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-2016-8743	128.238.66.31	443	12/19/2019, 5:29:34 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-2015-3185	216.165.49.28	443	12/19/2019, 2:46:05 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	216.165.49.28	443	12/19/2019, 2:46:05 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	216.165.49.28	443	12/19/2019, 2:46:05 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-2015-3183	216.165.49.28	443	12/19/2019, 2:46:05 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-7529	34.192.16.97	443	12/18/2019, 9:19:06 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-2016-4450	34.192.16.97	443	12/18/2019, 9:19:06 PM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2015-3183	216.165.47.16	443	12/18/2019, 8:29:58 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-0226	216.165.47.16	443	12/18/2019, 8:29:58 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	216.165.47.16	443	12/18/2019, 8:29:58 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-2015-3185	216.165.47.16	443	12/18/2019, 8:29:58 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	216.165.78.14	443	12/18/2019, 7:48:02 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-2016-8743	128.122.49.75	443	12/18/2019, 5:48:24 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-2014-0226	128.122.49.75	443	12/18/2019, 5:48:24 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3670	128.122.49.75	443	12/18/2019, 5:48:24 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2014-3597	128.122.49.75	443	12/18/2019, 5:48:24 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-3185	128.122.49.75	443	12/18/2019, 5:48:24 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-0232	128.122.49.75	443	12/18/2019, 5:48:24 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2017-3736	128.122.49.75	443	12/18/2019, 5:48:24 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.49.75	443	12/18/2019, 5:48:24 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.75	443	12/18/2019, 5:48:24 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	128.122.49.75	443	12/18/2019, 5:48:24 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	128.122.49.28	443	12/18/2019, 5:42:11 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	128.122.49.28	443	12/18/2019, 5:42:11 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	128.122.49.28	443	12/18/2019, 5:42:11 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3183	128.122.49.28	443	12/18/2019, 5:42:11 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.49.28	443	12/18/2019, 5:42:11 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.49.28	443	12/18/2019, 5:42:11 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-2017-3738	128.122.49.28	443	12/18/2019, 5:42:11 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	91.230.41.37	443	12/18/2019, 3:08:31 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-2016-8743	128.122.4.241	443	12/18/2019, 1:52:00 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-2015-3185	34.194.136.93	443	12/17/2019, 6:23:05 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	34.194.136.93	443	12/17/2019, 6:23:05 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	34.194.136.93	443	12/17/2019, 6:23:05 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-8743	128.122.109.122	443	12/17/2019, 6:16:51 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-2014-3566	128.122.40.84	995	12/17/2019, 5:19:31 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-0204	128.122.40.84	995	12/17/2019, 5:19:31 PM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-4000	128.122.40.84	995	12/17/2019, 5:19:31 PM	5/20/2015, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.				
CVE-2016-8743	128.122.87.169	443	12/17/2019, 5:04:55 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-2017-3737	128.122.238.100	443	12/17/2019, 4:48:06 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2017-3738	128.122.238.100	443	12/17/2019, 4:48:06 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	216.165.47.56	443	12/17/2019, 4:02:34 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-2017-3736	128.122.149.150	443	12/17/2019, 11:38:01 AM	11/2/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	128.122.149.150	443	12/17/2019, 11:38:01 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.149.150	443	12/17/2019, 11:38:01 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-2017-3738	128.122.149.150	443	12/17/2019, 11:38:01 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.122.149.36	443	12/17/2019, 10:58:56 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-2016-8743	91.230.41.215	443	12/17/2019, 10:57:38 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-2017-3736	128.122.149.108	443	12/17/2019, 10:46:58 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.149.108	443	12/17/2019, 10:46:58 AM	12/7/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.149.108	443	12/17/2019, 10:46:58 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.149.108	443	12/17/2019, 10:46:58 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-2016-8743	128.238.38.77	443	12/17/2019, 7:05:43 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-2016-8743	128.122.109.120	443	12/17/2019, 4:20:36 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-2015-0204	128.122.40.84	993	12/17/2019, 3:43:53 AM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.130.104	80	12/14/2019, 5:13:24 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-2016-8743	128.122.130.10	80	12/14/2019, 5:13:14 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-2014-3597	128.122.130.72	80	12/14/2019, 5:08:03 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-3670	128.122.130.72	80	12/14/2019, 5:08:03 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.122.130.72	80	12/14/2019, 5:08:03 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-2014-3597	128.122.130.129	80	12/14/2019, 5:05:54 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-0232	128.122.130.129	80	12/14/2019, 5:05:54 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2015-0204	128.122.128.25	443	12/14/2019, 5:00:18 AM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-4000	128.122.128.25	443	12/14/2019, 5:00:18 AM	5/20/2015, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.				
CVE-2016-8743	216.165.108.10	80	12/14/2019, 3:48:25 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-2014-3566	195.113.94.137	443	12/13/2019, 8:03:04 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.107.83	80	12/13/2019, 7:40:25 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-2016-8743	91.230.41.211	80	12/13/2019, 4:02:00 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-2017-7529	34.192.16.97	80	12/13/2019, 3:29:34 PM	7/13/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2016-4450	34.192.16.97	80	12/13/2019, 3:29:34 PM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-0800	128.122.174.6	443	12/13/2019, 2:01:04 PM	3/1/2016, 12:00:00 AM
Vulnerability Description : The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.				
CVE-2014-3566	128.122.174.6	443	12/13/2019, 2:01:04 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2017-7529	128.122.180.64	80	12/13/2019, 12:40:03 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-2016-8743	128.122.149.148	80	12/13/2019, 11:22:36 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	128.122.59.145	80	12/13/2019, 10:11:39 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-2016-4450	128.122.59.145	80	12/13/2019, 10:11:39 AM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-8743	128.122.85.53	80	12/13/2019, 3:39:09 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-2014-3566	128.122.149.68	443	12/13/2019, 3:19:23 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.35.88	80	12/13/2019, 2:51:01 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-2016-8743	216.165.113.70	80	12/13/2019, 1:27:44 AM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2014-3566	128.122.149.154	443	12/12/2019, 11:13:23 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.130.228	80	12/12/2019, 11:08:35 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-2016-8743	128.122.49.123	80	12/12/2019, 10:56:41 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-2014-3566	128.122.149.173	443	12/12/2019, 10:51:10 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.121.220	443	12/12/2019, 9:40:53 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.238.63.25	80	12/12/2019, 7:14:34 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-2016-8743	128.122.4.241	80	12/12/2019, 6:01:08 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-2016-0800	128.122.120.77	443	12/12/2019, 1:06:06 PM	3/1/2016, 12:00:00 AM
Vulnerability Description : The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.				
CVE-2014-3566	128.122.120.77	443	12/12/2019, 1:06:06 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.117.5	443	12/12/2019, 10:05:43 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3185	34.194.136.93	80	12/12/2019, 8:41:51 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	34.194.136.93	80	12/12/2019, 8:41:51 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	34.194.136.93	80	12/12/2019, 8:41:51 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-2016-0703	128.122.87.234	80	12/12/2019, 7:36:49 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-2015-3195	128.122.87.234	80	12/12/2019, 7:36:49 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2014-3566	128.122.2.28	443	12/12/2019, 7:14:45 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.209.96	443	12/12/2019, 6:58:46 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.235.5	80	12/12/2019, 4:36:56 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-2016-8743	128.122.11.92	80	12/12/2019, 3:51:43 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-2014-0226	128.122.11.92	80	12/12/2019, 3:51:43 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-3183	128.122.11.92	80	12/12/2019, 3:51:43 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.11.92	80	12/12/2019, 3:51:43 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.149.36	80	12/11/2019, 11:51:13 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-2016-8743	128.122.149.129	80	12/11/2019, 11:38:47 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-2016-8743	128.122.230.133	80	12/11/2019, 11:06:58 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-2014-0226	128.122.108.98	80	12/11/2019, 9:35:23 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.108.98	80	12/11/2019, 9:35:23 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.108.98	80	12/11/2019, 9:35:23 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-2015-3185	128.122.108.98	80	12/11/2019, 9:35:23 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-3566	128.122.4.241	443	12/11/2019, 7:52:37 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-3566	128.122.5.5	443	12/11/2019, 7:45:15 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.238.38.77	80	12/11/2019, 6:09:52 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-2016-8743	128.122.109.9	80	12/11/2019, 3:48:07 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-2015-3183	128.122.108.128	80	12/11/2019, 3:23:37 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.108.128	80	12/11/2019, 3:23:37 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-3566	128.122.149.82	443	12/11/2019, 11:13:37 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.149.120	443	12/11/2019, 10:57:15 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.83.79	443	12/10/2019, 9:03:59 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.149.33	443	12/10/2019, 2:48:11 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.149.108	443	12/10/2019, 2:33:47 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.149.150	443	12/10/2019, 2:23:53 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-3566	128.122.108.64	443	12/10/2019, 10:56:53 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.108.59	443	12/10/2019, 10:56:02 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.108.121	443	12/10/2019, 2:29:33 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-0777	128.122.253.80	22	12/9/2019, 7:10:29 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-2016-0777	216.165.113.217	22	12/9/2019, 6:53:46 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-2016-0777	128.122.161.197	22	12/9/2019, 6:29:51 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-2016-0777	128.122.90.152	22	12/9/2019, 5:32:20 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-2016-0777	128.122.90.72	22	12/9/2019, 5:31:14 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-2016-0777	128.122.88.5	22	12/9/2019, 4:47:27 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-2016-0777	128.122.149.62	22	12/9/2019, 1:09:02 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-2016-0777	128.238.63.25	22	12/9/2019, 8:24:17 AM	1/14/2016, 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-2016-0777	128.122.4.242	22	12/9/2019, 8:05:56 AM	4/1/2016, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2016-0777	128.122.251.235	22	12/9/2019, 6:56:23 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-2016-8743	159.65.160.172	443	12/9/2019, 4:56:34 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-2016-0777	128.122.238.18	22	12/9/2019, 4:44:49 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-2016-8743	128.238.63.25	443	12/9/2019, 4:25:20 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-2016-0777	128.122.149.79	22	12/9/2019, 2:39:17 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-2016-0777	128.122.149.123	22	12/9/2019, 2:35:33 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-2016-0777	128.122.149.76	22	12/9/2019, 2:34:15 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-2016-0777	128.122.108.87	22	12/9/2019, 1:56:42 AM	1/14/2016, 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-2016-0777	192.86.139.71	22	12/9/2019, 12:53:48 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-2016-0777	107.180.61.237	22	12/8/2019, 11:39:23 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-2015-3185	128.122.49.52	8443	11/26/2019, 8:54:05 AM	7/20/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.49.52	8443	11/26/2019, 8:54:05 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	128.122.49.52	8443	11/26/2019, 8:54:05 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	128.122.49.52	8443	11/26/2019, 8:54:05 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.49.52	8443	11/26/2019, 8:54:05 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.49.52	8443	11/26/2019, 8:54:05 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.49.52	8443	11/26/2019, 8:54:05 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-2016-0777	195.113.94.167	22	11/26/2019, 5:49:59 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-2016-0777	128.238.7.158	22	11/26/2019, 4:52:22 AM	4/1/2016, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2016-0777	195.113.94.141	22	11/26/2019, 3:58:16 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-2017-5650	128.122.108.165	8080	11/25/2019, 3:45:50 PM	4/17/2017, 12:00:00 AM
Vulnerability Description : In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the handling of an HTTP/2 GOAWAY frame for a connection did not close streams associated with that connection that were currently waiting for a WINDOW_UPDATE before allowing the application to write more data. These waiting streams each consumed a thread. A malicious client could therefore construct a series of HTTP/2 requests that would consume all available processing threads.				
CVE-2017-5664	128.122.108.165	8080	11/25/2019, 3:45:50 PM	6/6/2017, 12:00:00 AM
Vulnerability Description : The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.				
CVE-2017-5647	128.122.108.165	8080	11/25/2019, 3:45:50 PM	4/17/2017, 12:00:00 AM
Vulnerability Description : A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.				
CVE-2017-7675	128.122.108.165	8080	11/25/2019, 3:45:50 PM	8/10/2017, 12:00:00 AM
Vulnerability Description : The HTTP/2 implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M21 and 8.5.0 to 8.5.15 bypassed a number of security checks that prevented directory traversal attacks. It was therefore possible to bypass security constraints using a specially crafted URL.				
CVE-2015-3195	128.122.108.165	443	11/15/2019, 9:07:54 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2016-8743	128.122.108.165	443	11/15/2019, 9:07:54 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-2015-3194	128.122.108.165	443	11/15/2019, 9:07:54 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2015-3197	128.122.108.165	443	11/15/2019, 9:07:54 AM	2/14/2016, 12:00:00 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-0703	128.122.128.69	443	11/14/2019, 9:00:26 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-2016-8743	128.122.128.69	443	11/14/2019, 9:00:26 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-2016-8743	216.165.78.8	443	11/14/2019, 1:07:10 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-2017-7529	128.122.85.82	443	11/13/2019, 8:29:40 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-2014-3556	128.122.85.82	443	11/13/2019, 8:29:40 PM	12/29/2014, 12:00:00 AM
Vulnerability Description : The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.				
CVE-2016-4450	128.122.85.82	443	11/13/2019, 8:29:40 PM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-0800	128.122.107.141	990	11/13/2019, 5:54:53 PM	3/1/2016, 12:00:00 AM
Vulnerability Description : The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.				
CVE-2014-3566	128.122.107.141	990	11/13/2019, 5:54:53 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.157.182	80	11/10/2019, 7:16:49 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-2014-3566	128.122.123.27	443	11/10/2019, 2:29:12 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.149.6	80	11/10/2019, 12:20:58 PM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2015-4000	128.122.128.69	443	11/10/2019, 11:29:30 AM	5/20/2015, 12:00:00 AM
Vulnerability Description : The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.				
CVE-2015-0204	128.122.128.69	443	11/10/2019, 11:29:30 AM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.128.69	80	11/10/2019, 11:04:18 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-2016-0703	128.122.128.69	80	11/10/2019, 11:04:18 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-2016-8743	128.122.93.210	80	11/9/2019, 10:29:26 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-2016-8743	128.122.68.222	80	11/9/2019, 8:23:10 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-2016-4450	128.122.85.82	80	11/9/2019, 7:18:49 AM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2017-7529	128.122.85.82	80	11/9/2019, 7:18:49 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-2014-3556	128.122.85.82	80	11/9/2019, 7:18:49 AM	12/29/2014, 12:00:00 AM
Vulnerability Description : The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.				
CVE-2014-3566	128.122.30.18	443	11/8/2019, 11:31:36 AM	10/14/2014, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.238.138	443	11/8/2019, 11:09:08 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2017-7529	35.174.218.100	443	11/8/2019, 1:17:26 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-2017-7529	128.238.63.19	443	11/7/2019, 12:55:13 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-2016-0777	128.122.84.114	22	11/7/2019, 6:31:28 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-2016-0777	128.122.45.62	22	11/7/2019, 4:35:34 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-2014-3566	128.122.40.84	143	11/7/2019, 4:05:57 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-0777	128.122.7.133	22	11/7/2019, 2:16:36 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-2016-0777	195.113.94.168	22	11/6/2019, 11:53:13 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-2016-0777	128.122.93.210	22	11/6/2019, 10:55:05 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-2016-0777	128.122.2.185	22	11/6/2019, 8:47:46 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-2015-0204	128.122.40.84	110	11/6/2019, 8:04:33 AM	1/8/2015, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-3566	128.122.40.84	110	11/6/2019, 8:04:33 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-0777	195.113.94.166	22	10/22/2019, 2:00:50 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-2017-7529	128.238.63.19	80	10/19/2019, 8:42:49 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-2015-3183	128.238.182.18	80	10/19/2019, 5:33:28 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3670	128.238.182.18	80	10/19/2019, 5:33:28 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3737	128.238.182.18	80	10/19/2019, 5:33:28 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-0232	128.238.182.18	80	10/19/2019, 5:33:28 PM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-3597	128.238.182.18	80	10/19/2019, 5:33:28 PM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2017-3736	128.238.182.18	80	10/19/2019, 5:33:28 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.238.182.18	80	10/19/2019, 5:33:28 PM	12/7/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.238.182.18	80	10/19/2019, 5:33:28 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.238.182.18	80	10/19/2019, 5:33:28 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-2015-3185	128.238.182.18	80	10/19/2019, 5:33:28 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-7529	128.238.147.222	80	10/19/2019, 3:49:50 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-2017-7529	35.174.218.100	80	10/19/2019, 5:48:38 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-2016-8743	180.168.176.151	443	10/16/2019, 10:46:08 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-2016-8743	128.122.157.182	443	10/16/2019, 3:35:49 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-2015-3185	128.122.217.176	443	10/16/2019, 1:51:03 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	128.122.217.176	443	10/16/2019, 1:51:03 PM	12/7/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2014-0226	128.122.217.176	443	10/16/2019, 1:51:03 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.149.6	443	10/16/2019, 6:49:41 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-2014-3670	128.122.4.236	443	10/16/2019, 4:53:03 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2015-3183	128.122.4.236	443	10/16/2019, 4:53:03 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.4.236	443	10/16/2019, 4:53:03 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-2014-3597	128.122.4.236	443	10/16/2019, 4:53:03 AM	8/22/2014, 12:00:00 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2017-3736	128.122.4.236	443	10/16/2019, 4:53:03 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.4.236	443	10/16/2019, 4:53:03 AM	12/7/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.4.236	443	10/16/2019, 4:53:03 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-0232	128.122.4.236	443	10/16/2019, 4:53:03 AM	1/27/2015, 12:00:00 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3737	128.122.4.236	443	10/16/2019, 4:53:03 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.122.4.236	443	10/16/2019, 4:53:03 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-4450	128.238.147.222	443	10/15/2019, 11:57:20 PM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2017-7529	128.238.147.222	443	10/15/2019, 11:57:20 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-2016-4450	91.230.41.28	443	10/15/2019, 7:10:46 AM	6/7/2016, 12:00:00 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2017-7529	91.230.41.28	443	10/15/2019, 7:10:46 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-2015-3183	216.165.85.213	443	10/15/2019, 2:44:34 AM	7/20/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	216.165.85.213	443	10/15/2019, 2:44:34 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	216.165.85.213	443	10/15/2019, 2:44:34 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-2017-3737	216.165.85.213	443	10/15/2019, 2:44:34 AM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	216.165.85.213	443	10/15/2019, 2:44:34 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	216.165.85.213	443	10/15/2019, 2:44:34 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	216.165.85.213	443	10/15/2019, 2:44:34 AM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	216.165.85.216	443	10/14/2019, 7:34:03 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-2015-3185	216.165.85.216	443	10/14/2019, 7:34:03 PM	7/20/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	216.165.85.216	443	10/14/2019, 7:34:03 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	216.165.85.216	443	10/14/2019, 7:34:03 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3566	216.165.85.201	465	10/13/2019, 12:19:58 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.83.82	443	10/12/2019, 1:59:32 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.83.71	443	10/12/2019, 1:42:53 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.83.73	443	10/12/2019, 1:41:29 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-3185	128.238.64.107	80	10/12/2019, 12:21:46 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.238.64.107	80	10/12/2019, 12:21:46 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.238.64.107	80	10/12/2019, 12:21:46 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.238.63.7	80	10/11/2019, 11:11:23 PM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2016-8743	128.122.149.60	80	10/11/2019, 11:07:57 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-2016-8743	128.122.2.69	80	10/11/2019, 7:42:39 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-2015-3183	216.165.86.17	80	10/11/2019, 12:16:36 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	216.165.86.17	80	10/11/2019, 12:16:36 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	216.165.86.17	80	10/11/2019, 12:16:36 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	216.165.86.17	80	10/11/2019, 12:16:36 PM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	216.165.86.17	80	10/11/2019, 12:16:36 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.130.205	80	10/11/2019, 11:13:19 AM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2014-3566	216.165.85.217	443	10/11/2019, 10:09:20 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.85.208	443	10/11/2019, 9:53:24 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.85.206	443	10/11/2019, 9:52:56 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.85.203	443	10/11/2019, 9:43:01 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	128.122.54.78	443	10/11/2019, 8:15:15 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-3566	216.165.94.244	443	10/11/2019, 5:00:34 AM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2015-3183	128.122.4.236	80	10/11/2019, 2:57:57 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.4.236	80	10/11/2019, 2:57:57 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.4.236	80	10/11/2019, 2:57:57 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-2017-3737	128.122.4.236	80	10/11/2019, 2:57:57 AM	12/7/2017, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2014-3670	128.122.4.236	80	10/11/2019, 2:57:57 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.122.130.177	80	10/11/2019, 1:46:05 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-2016-8743	128.122.130.116	80	10/11/2019, 1:34:48 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-2016-8743	128.122.130.32	80	10/11/2019, 1:32:40 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-2016-8743	128.122.130.129	80	10/11/2019, 1:32:22 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-2014-3670	128.122.130.129	80	10/11/2019, 1:32:22 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.122.130.144	80	10/11/2019, 1:27:53 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-2016-8743	128.122.49.114	80	10/11/2019, 12:44:55 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-2016-8743	128.122.130.6	80	10/10/2019, 10:51:59 PM	7/27/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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-2016-8743	216.165.4765	80	10/10/2019, 9:01:12 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-2014-3566	128.122.4.236	443	10/10/2019, 1:00:38 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.31.92	80	10/10/2019, 12:49:03 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-2015-3185	128.122.108.82	80	10/10/2019, 5:29:34 AM	7/20/2015, 12:00:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.108.82	80	10/10/2019, 5:29:34 AM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.108.82	80	10/10/2019, 5:29:34 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-2014-3566	216.165.86.168	443	10/9/2019, 5:26:08 PM	10/14/2014, 12:00:00 AM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2016-8743	128.122.108.91	80	10/9/2019, 2:03:35 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-2016-8743	128.122.108.121	80	10/9/2019, 1:52:41 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-2017-3737	128.122.108.128	80	10/9/2019, 1:50:10 PM	12/7/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2017-3738	128.122.108.128	80	10/9/2019, 1:50:10 PM	12/7/2017, 12:00:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 11.0 at this time. The fix will be included in OpenSSL 11.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.108.128	80	10/9/2019, 1:50:10 PM	7/20/2014, 12:00:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.108.128	80	10/9/2019, 1:50:10 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-2017-3736	128.122.108.128	80	10/9/2019, 1:50:10 PM	11/2/2017, 12:00:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.70.189	80	10/9/2019, 1:15:54 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-2015-3197	128.122.108.165	80	10/9/2019, 11:59:55 AM	2/14/2016, 12:00:00 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2015-3195	128.122.108.165	80	10/9/2019, 11:59:55 AM	12/6/2015, 12:00:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				

## ! Low-Severity Vulnerability in Last Observation

-0.3 SCORE IMPACT

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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.

## 24 findings

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-3956	216.165.85.201	587	6/4/2014, 12:00:00 AM	3/11/2020, 9:27:21 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.128.117	587	6/4/2014, 12:00:00 AM	3/11/2020, 8:23:27 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.50	587	6/4/2014, 12:00:00 AM	3/11/2020, 8:11:27 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.100	587	6/4/2014, 12:00:00 AM	3/11/2020, 8:10:04 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.97	587	6/4/2014, 12:00:00 AM	3/11/2020, 8:09:56 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.47.33	587	6/4/2014, 12:00:00 AM	3/11/2020, 4:55:59 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.97	465	6/4/2014, 12:00:00 AM	3/11/2020, 8:06:59 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.100	465	6/4/2014, 12:00:00 AM	3/11/2020, 8:06:42 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.47.10	25	6/4/2014, 12:00:00 AM	3/5/2020, 1:14:31 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.85.207	25	6/4/2014, 12:00:00 AM	3/5/2020, 12:19:30 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2002-1827	128.122.112.176	25	12/31/2002, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : Sendmail 8.9.0 through 8.12.3 allows local users to cause a denial of service by obtaining an exclusive lock on the (1) alias, (2) map, (3) statistics, and (4) pid files.				
CVE-2014-3956	128.238.66.173	25	6/4/2014, 12:00:00 AM	3/5/2020, 10:58:01 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.26.240	25	6/4/2014, 12:00:00 AM	3/5/2020, 10:36:33 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.50	25	6/4/2014, 12:00:00 AM	3/5/2020, 10:01:55 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.97	25	6/4/2014, 12:00:00 AM	3/5/2020, 9:58:57 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.100	25	6/4/2014, 12:00:00 AM	3/5/2020, 9:57:37 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.17	25	6/4/2014, 12:00:00 AM	3/5/2020, 9:56:25 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.238.66.35	25	6/4/2014, 12:00:00 AM	3/5/2020, 9:12:46 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.238.66.55	25	6/4/2014, 12:00:00 AM	3/5/2020, 9:11:01 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.128.117	25	6/4/2014, 12:00:00 AM	3/5/2020, 8:43:07 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-3956	128.122.60.87	25	6/4/2014, 12:00:00 AM	3/5/2020, 8:05:57 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.238.66.31	25	6/4/2014, 12:00:00 AM	3/5/2020, 6:34:07 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.47.32	25	6/4/2014, 12:00:00 AM	3/5/2020, 5:25:24 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	216.165.85.200	25	6/4/2014, 12:00:00 AM	2/5/2020, 11:36:57 PM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				

## !!! High-Severity Vulnerability in Last Observation

-1.1 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.

### 160 findings

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2009-4565	128.122.128.10	587	1/4/2010, 12:00:00 AM	3/11/2020, 7:34:22 PM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2006-0058	128.122.128.10	587	3/22/2006, 12:00:00 AM	3/11/2020, 7:34:22 PM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2009-4565	193.175.54.5	587	1/4/2010, 12:00:00 AM	3/11/2020, 6:08:12 PM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2006-0058	193.175.54.5	587	3/22/2006, 12:00:00 AM	3/11/2020, 6:08:12 PM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2014-3669	128.122.49.75	443	10/29/2014, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.75	443	7/9/2014, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.49.75	443	1/2/2015, 12:00:00 AM	3/10/2020, 2:16:45 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-2014-3515	128.122.49.17	443	7/9/2014, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.49.17	443	10/29/2014, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.49.17	443	1/2/2015, 12:00:00 AM	3/10/2020, 2:15:38 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-2014-3669	128.122.120.72	443	10/29/2014, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.120.72	443	7/9/2014, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.120.72	443	1/2/2015, 12:00:00 AM	3/10/2020, 11:58:17 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2011-3268	128.238.66.55	443	8/25/2011, 12:00:00 AM	3/10/2020, 11:29:05 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-2014-9427	128.238.66.55	443	1/2/2015, 12:00:00 AM	3/10/2020, 11:29:05 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-2014-3669	128.122.4.12	443	10/29/2014, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.4.12	443	7/9/2014, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.4.12	443	1/2/2015, 12:00:00 AM	3/10/2020, 9:49:39 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-2014-9427	128.122.128.72	443	1/2/2015, 12:00:00 AM	3/10/2020, 9:42:02 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-2014-9427	128.122.128.25	443	1/2/2015, 12:00:00 AM	3/10/2020, 9:39:23 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-2014-3669	128.238.26.32	80	10/29/2014, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.238.26.32	80	7/9/2014, 12:00:00 AM	3/10/2020, 8:51:15 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.238.26.32	80	1/2/2015, 12:00:00 AM	3/10/2020, 8:51:15 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-2015-2331	128.238.63.75	443	3/30/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Integer overflow in the _zip_cdir_new function in zip dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.				
CVE-2014-8142	128.238.63.75	443	12/20/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.				
CVE-2014-9653	128.238.63.75	443	3/30/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.				
CVE-2015-2301	128.238.63.75	443	3/30/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.				
CVE-2014-9427	128.238.63.75	443	1/2/2015, 12:00:00 AM	3/10/2020, 4:42:31 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-2014-3515	128.238.63.75	443	7/9/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2015-3307	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.				
CVE-2015-4026	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-4022	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.				
CVE-2015-3329	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.				
CVE-2014-3669	128.238.63.75	443	10/29/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2015-4025	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2014-9705	128.238.63.75	443	3/30/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2014-9427	128.122.128.34	443	1/2/2015, 12:00:00 AM	3/10/2020, 3:32:38 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-2011-3268	128.238.66.31	443	8/25/2011, 12:00:00 AM	3/10/2020, 2:29:05 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-2014-9427	128.238.66.31	443	1/2/2015, 12:00:00 AM	3/10/2020, 2:29:05 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-2011-3268	128.238.66.31	80	8/25/2011, 12:00:00 AM	3/10/2020, 1:37:40 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-2014-9427	128.238.66.31	80	1/2/2015, 12:00:00 AM	3/10/2020, 1:37:40 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-2014-3669	91.230.41.214	80	10/29/2014, 12:00:00 AM	3/10/2020, 12:02:20 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	91.230.41.214	80	1/2/2015, 12:00:00 AM	3/10/2020, 12:02:20 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-2014-3515	91.230.41.214	80	7/9/2014, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.238.63.10	80	1/2/2015, 12:00:00 AM	3/10/2020, 12:00:29 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-2014-3669	128.238.63.10	80	10/29/2014, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.238.63.10	80	7/9/2014, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.238.182.23	80	7/9/2014, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.238.182.23	80	10/29/2014, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.238.182.23	80	1/2/2015, 12:00:00 AM	3/9/2020, 11:35:47 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-2014-3515	128.122.49.27	443	7/9/2014, 12:00:00 AM	3/9/2020, 11:21:50 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-3669	128.122.49.27	443	10/29/2014, 12:00:00 AM	3/9/2020, 11:21:50 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.49.27	443	1/2/2015, 12:00:00 AM	3/9/2020, 11:21:50 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-2014-9427	216.165.26.109	443	1/2/2015, 12:00:00 AM	3/9/2020, 9:43:02 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-2014-3669	216.165.26.109	443	10/29/2014, 12:00:00 AM	3/9/2020, 9:43:02 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	216.165.26.109	443	7/9/2014, 12:00:00 AM	3/9/2020, 9:43:02 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2015-4022	128.238.63.75	80	6/9/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.				
CVE-2015-3329	128.238.63.75	80	6/9/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.				
CVE-2014-8142	128.238.63.75	80	12/20/2014, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.				
CVE-2015-2331	128.238.63.75	80	3/30/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.				
CVE-2014-9427	128.238.63.75	80	1/2/2015, 12:00:00 AM	3/9/2020, 6:46:43 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-3515	128.238.63.75	80	7/9/2014, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2015-4026	128.238.63.75	80	6/9/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2014-3669	128.238.63.75	80	10/29/2014, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9705	128.238.63.75	80	3/30/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2015-4025	128.238.63.75	80	6/9/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-3307	128.238.63.75	80	6/9/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.				
CVE-2014-9653	128.238.63.75	80	3/30/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.				
CVE-2015-2301	128.238.63.75	80	3/30/2015, 12:00:00 AM	3/9/2020, 6:46:43 PM
Vulnerability Description : Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.				
CVE-2014-3515	128.122.130.121	443	7/9/2014, 12:00:00 AM	3/9/2020, 6:30:56 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.130.121	443	10/29/2014, 12:00:00 AM	3/9/2020, 6:30:56 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.130.121	443	1/2/2015, 12:00:00 AM	3/9/2020, 6:30:56 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2011-3268	128.238.66.55	80	8/25/2011, 12:00:00 AM	3/9/2020, 5:45:06 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-2014-9427	128.238.66.55	80	1/2/2015, 12:00:00 AM	3/9/2020, 5:45:06 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-2014-9427	128.238.149.48	80	1/2/2015, 12:00:00 AM	3/9/2020, 5:37:25 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-2014-3515	128.238.63.11	80	7/9/2014, 12:00:00 AM	3/9/2020, 4:32:37 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.238.63.11	80	1/2/2015, 12:00:00 AM	3/9/2020, 4:32:37 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-2014-3669	128.238.63.11	80	10/29/2014, 12:00:00 AM	3/9/2020, 4:32:37 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3669	128.238.182.23	443	10/29/2014, 12:00:00 AM	3/9/2020, 3:56:55 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.238.182.23	443	1/2/2015, 12:00:00 AM	3/9/2020, 3:56:55 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-2014-3515	128.238.182.23	443	7/9/2014, 12:00:00 AM	3/9/2020, 3:56:55 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.86.187	443	10/29/2014, 12:00:00 AM	3/9/2020, 3:39:32 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.86.187	443	1/2/2015, 12:00:00 AM	3/9/2020, 3:39:32 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-2014-3515	128.122.86.187	443	7/9/2014, 12:00:00 AM	3/9/2020, 3:39:32 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.86.183	443	1/2/2015, 12:00:00 AM	3/9/2020, 3:37:46 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-2014-3669	128.122.49.20	80	10/29/2014, 12:00:00 AM	3/7/2020, 7:40:25 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.20	80	7/9/2014, 12:00:00 AM	3/7/2020, 7:40:25 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.49.20	80	1/2/2015, 12:00:00 AM	3/7/2020, 7:40:25 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-2014-3515	128.122.49.75	80	7/9/2014, 12:00:00 AM	3/7/2020, 7:34:39 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.49.75	80	1/2/2015, 12:00:00 AM	3/7/2020, 7:34:39 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2014-3669	128.122.49.75	80	10/29/2014, 12:00:00 AM	3/7/2020, 7:34:39 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3669	128.122.49.17	80	10/29/2014, 12:00:00 AM	3/7/2020, 7:31:45 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.49.17	80	1/2/2015, 12:00:00 AM	3/7/2020, 7:31:45 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-2014-3515	128.122.49.17	80	7/9/2014, 12:00:00 AM	3/7/2020, 7:31:45 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.4.12	80	7/9/2014, 12:00:00 AM	3/7/2020, 3:16:51 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.4.12	80	1/2/2015, 12:00:00 AM	3/7/2020, 3:16:51 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-2014-3669	128.122.4.12	80	10/29/2014, 12:00:00 AM	3/7/2020, 3:16:51 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3669	128.122.4.48	80	10/29/2014, 12:00:00 AM	3/7/2020, 3:11:58 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.4.48	80	7/9/2014, 12:00:00 AM	3/7/2020, 3:11:58 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2014-9427	128.122.4.48	80	1/2/2015, 12:00:00 AM	3/7/2020, 3:11:58 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-2014-9427	128.122.128.25	80	1/2/2015, 12:00:00 AM	3/7/2020, 3:10:47 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-2014-9427	128.122.128.72	80	1/2/2015, 12:00:00 AM	3/7/2020, 3:07:46 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-2014-3515	128.122.8.38	80	7/9/2014, 12:00:00 AM	3/6/2020, 10:30:04 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.8.38	80	1/2/2015, 12:00:00 AM	3/6/2020, 10:30:04 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-2014-3669	128.122.8.38	80	10/29/2014, 12:00:00 AM	3/6/2020, 10:30:04 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.35.88	80	1/2/2015, 12:00:00 AM	3/6/2020, 5:15:01 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-2011-3268	128.122.35.88	80	8/25/2011, 12:00:00 AM	3/6/2020, 5:15:01 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-2014-8626	128.122.35.88	80	11/22/2014, 12:00:00 AM	3/6/2020, 5:15:01 PM
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-2014-9427	128.122.49.27	80	1/2/2015, 12:00:00 AM	3/6/2020, 3:28:52 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2014-3669	128.122.49.27	80	10/29/2014, 12:00:00 AM	3/6/2020, 3:28:52 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.27	80	7/9/2014, 12:00:00 AM	3/6/2020, 3:28:52 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.235.5	80	1/2/2015, 12:00:00 AM	3/6/2020, 1:48:58 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-2014-9427	128.122.130.72	80	1/2/2015, 12:00:00 AM	3/6/2020, 10:55:41 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-2014-3515	128.122.130.72	80	7/9/2014, 12:00:00 AM	3/6/2020, 10:55:41 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.130.72	80	10/29/2014, 12:00:00 AM	3/6/2020, 10:55:41 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.86.187	80	1/2/2015, 12:00:00 AM	3/6/2020, 7:46:33 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-2014-3669	128.122.86.187	80	10/29/2014, 12:00:00 AM	3/6/2020, 7:46:33 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.86.187	80	7/9/2014, 12:00:00 AM	3/6/2020, 7:46:33 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.86.183	80	1/2/2015, 12:00:00 AM	3/6/2020, 7:37:38 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-2002-2261	128.122.112.176	25	12/31/2002, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : Sendmail 8.9.0 through 8.12.6 allows remote attackers to bypass relaying restrictions enforced by the 'check_relay' function by spoofing a blank DNS hostname.				
CVE-2009-4565	128.122.112.176	25	1/4/2010, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2002-0906	128.122.112.176	25	10/4/2002, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : Buffer overflow in Sendmail before 8.12.5, when configured to use a custom DNS map to query TXT records, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a malicious DNS server.				
CVE-2002-1337	128.122.112.176	25	3/7/2003, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : Buffer overflow in Sendmail 5.7.9 to 8.12.7 allows remote attackers to execute arbitrary code via certain formatted address fields, related to sender and recipient header comments as processed by the crackaddr function of headers.c.				
CVE-2003-0161	128.122.112.176	25	4/2/2003, 12:00:00 AM	3/5/2020, 12:06:20 PM
Vulnerability Description : The prescan() function in the address parser (parseaddr.c) in Sendmail before 8.12.9 does not properly handle certain conversions from char and int types, which can cause a length check to be disabled when Sendmail misinterprets an input value as a special "NOCHAR" control value, allowing attackers to cause a denial of service and possibly execute arbitrary code via a buffer overflow attack using messages, a different vulnerability than CVE-2002-1337.				
CVE-2009-4565	128.238.66.35	25	1/4/2010, 12:00:00 AM	3/5/2020, 9:12:46 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2009-4565	128.238.66.55	25	1/4/2010, 12:00:00 AM	3/5/2020, 9:11:01 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2006-0058	128.122.128.2	25	3/22/2006, 12:00:00 AM	3/5/2020, 8:41:48 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2009-4565	128.122.128.2	25	1/4/2010, 12:00:00 AM	3/5/2020, 8:41:48 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2006-0058	128.122.128.10	25	3/22/2006, 12:00:00 AM	3/5/2020, 8:41:36 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2009-4565	128.122.128.10	25	1/4/2010, 12:00:00 AM	3/5/2020, 8:41:36 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2009-4565	193.175.54.5	25	1/4/2010, 12:00:00 AM	3/5/2020, 5:42:53 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2006-0058	193.175.54.5	25	3/22/2006, 12:00:00 AM	3/5/2020, 5:42:53 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2016-6515	128.122.224.5	22	8/7/2016, 12:00:00 AM	3/4/2020, 1:51:40 PM
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-2016-6515	128.122.250.27	22	8/7/2016, 12:00:00 AM	3/4/2020, 12:21:59 PM
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-2016-6515	128.122.141.21	22	8/7/2016, 12:00:00 AM	3/4/2020, 11:15:32 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-2011-3268	128.238.63.53	443	8/25/2011, 12:00:00 AM	2/16/2020, 11:45:03 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-2014-9427	128.238.63.53	443	1/2/2015, 12:00:00 AM	2/16/2020, 11:45:03 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-2014-8626	128.238.63.53	443	11/22/2014, 12:00:00 AM	2/16/2020, 11:45:03 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-2016-1908	193.146.139.122	22	4/11/2017, 12:00:00 AM	2/12/2020, 3:44:55 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.				
CVE-2016-6515	193.146.139.122	22	8/7/2016, 12:00:00 AM	2/12/2020, 3:44:55 PM
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-2016-6515	195.113.94.10	22	8/7/2016, 12:00:00 AM	2/12/2020, 12:03:23 PM
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-2016-1908	195.113.94.10	22	4/11/2017, 12:00:00 AM	2/12/2020, 12:03:23 PM
Vulnerability Description : The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.				
CVE-2014-9427	128.122.49.20	443	1/2/2015, 12:00:00 AM	2/12/2020, 1:42:47 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-2014-3669	128.122.49.20	443	10/29/2014, 12:00:00 AM	2/12/2020, 1:42:47 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.20	443	7/9/2014, 12:00:00 AM	2/12/2020, 1:42:47 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.238.63.51	443	1/2/2015, 12:00:00 AM	2/11/2020, 11:42:48 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-2011-3268	128.238.63.51	443	8/25/2011, 12:00:00 AM	2/11/2020, 11:42:48 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	128.238.63.51	443	11/22/2014, 12:00:00 AM	2/11/2020, 11:42:48 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-2014-3669	128.122.4.48	443	10/29/2014, 12:00:00 AM	2/11/2020, 11:14:29 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.4.48	443	1/2/2015, 12:00:00 AM	2/11/2020, 11:14:29 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-2014-3515	128.122.4.48	443	7/9/2014, 12:00:00 AM	2/11/2020, 11:14:29 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-8626	128.238.63.51	80	11/22/2014, 12:00:00 AM	2/8/2020, 10:31:48 PM
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-2014-9427	128.238.63.51	80	1/2/2015, 12:00:00 AM	2/8/2020, 10:31:48 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-2011-3268	128.238.63.51	80	8/25/2011, 12:00:00 AM	2/8/2020, 10:31:48 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-2014-8626	128.238.63.53	80	11/22/2014, 12:00:00 AM	2/8/2020, 5:47:38 PM
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-2011-3268	128.238.63.53	80	8/25/2011, 12:00:00 AM	2/8/2020, 5:47:38 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-2014-9427	128.238.63.53	80	1/2/2015, 12:00:00 AM	2/8/2020, 5:47:38 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-2014-3669	128.122.130.129	80	10/29/2014, 12:00:00 AM	2/6/2020, 9:32:14 PM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.130.129	80	1/2/2015, 12:00:00 AM	2/6/2020, 9:32:14 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2014-3515	128.122.130.129	80	7/9/2014, 12:00:00 AM	2/6/2020, 9:32:14 PM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				

## !!! High Severity CVEs Patching Cadence

-1.2 SCORE IMPACT

High severity vulnerability seen on network more than 30 days after CVE was published.

### Description

Based on scan data, the company had high severity CVE vulnerability that was open longer than 30 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 30 days. Details on each vulnerability are listed in the table below.

169 findings

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3669	128.122.120.72	443	1/12/2020, 1:56:40 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.120.72	443	1/12/2020, 1:56:40 AM	7/9/2014, 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-2014-9427	128.122.120.72	443	1/12/2020, 1:56:40 AM	1/2/2015, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2014-9705	216.165.26.240	443	1/11/2020, 7:13:30 PM	3/30/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.				
CVE-2015-4022	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2015-2331	216.165.26.240	443	1/11/2020, 7:13:30 PM	3/30/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the _zip_cdir_new function in zip dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.				
CVE-2015-4025	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-2301	216.165.26.240	443	1/11/2020, 7:13:30 PM	3/30/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.				
CVE-2015-3329	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.				
CVE-2015-4026	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-3307	216.165.26.240	443	1/11/2020, 7:13:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.				
CVE-2014-3515	128.122.49.17	443	1/11/2020, 5:57:03 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.49.17	443	1/11/2020, 5:57:03 PM	1/2/2015, 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-2014-3669	128.122.49.17	443	1/11/2020, 5:57:03 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3669	216.165.26.109	80	1/8/2020, 4:14:05 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-9427	216.165.26.109	80	1/8/2020, 4:14:05 AM	1/2/2015, 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-2014-3515	216.165.26.109	80	1/8/2020, 4:14:05 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2015-4022	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.				
CVE-2015-4025	216.165.26.240	80	1/7/2020, 8:09:30 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-2331	216.165.26.240	80	1/7/2020, 8:09:30 PM	3/30/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.				
CVE-2014-9427	128.122.49.20	80	1/7/2020, 9:49:45 AM	1/2/2015, 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-2014-3515	128.122.49.20	80	1/7/2020, 9:49:45 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.49.20	80	1/7/2020, 9:49:45 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2015-5722	128.238.32.22	53	1/6/2020, 9:20:54 AM	9/4/2015, 12:00:00 AM
Vulnerability Description : buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.				
CVE-2014-8500	128.238.32.22	53	1/6/2020, 9:20:54 AM	10/12/2014, 12:00:00 AM
Vulnerability Description : ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-2776	128.238.32.22	53	1/6/2020, 9:20:54 AM	9/28/2016, 12:00:00 AM
Vulnerability Description : buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.				
CVE-2015-5477	128.238.32.22	53	1/6/2020, 9:20:54 AM	7/29/2015, 12:00:00 AM
Vulnerability Description : named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.				
CVE-2016-10012	128.122.250.36	22	1/5/2020, 4:24:57 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	128.122.250.36	22	1/5/2020, 4:24:57 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	128.122.141.21	22	1/4/2020, 7:11:36 PM	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-2009-4565	216.165.85.201	465	12/19/2019, 4:20:00 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2014-3669	128.122.4.48	443	12/19/2019, 9:56:11 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.4.48	443	12/19/2019, 9:56:11 AM	1/2/2015, 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-2014-3515	128.122.4.48	443	12/19/2019, 9:56:11 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.128.25	443	12/19/2019, 9:55:52 AM	1/2/2015, 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-9427	128.238.66.31	443	12/19/2019, 5:29:34 AM	1/2/2015, 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-2011-3268	128.238.66.31	443	12/19/2019, 5:29:34 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-2014-9427	128.122.49.75	443	12/18/2019, 5:48:24 AM	1/2/2015, 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-2014-3669	128.122.49.75	443	12/18/2019, 5:48:24 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.75	443	12/18/2019, 5:48:24 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.130.72	80	12/14/2019, 5:08:03 AM	1/2/2015, 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-2014-3515	128.122.130.72	80	12/14/2019, 5:08:03 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.130.129	80	12/14/2019, 5:05:54 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-8626	128.122.35.88	80	12/13/2019, 2:51:01 AM	11/22/2014, 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-2011-3268	128.122.35.88	80	12/13/2019, 2:51:01 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-9427	128.122.35.88	80	12/13/2019, 2:51:01 AM	1/2/2015, 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-2014-9427	128.122.235.5	80	12/12/2019, 4:36:56 AM	1/2/2015, 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-2009-4565	128.238.66.55	25	12/10/2019, 12:12:33 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2017-5651	128.122.108.165	8080	11/25/2019, 3:45:50 PM	4/17/2017, 12:00:00 AM
Vulnerability Description : In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the refactoring of the HTTP connectors introduced a regression in the send file processing. If the send file processing completed quickly, it was possible for the Processor to be added to the processor cache twice. This could result in the same Processor being used for multiple requests which in turn could lead to unexpected errors and/or response mix-up.				
CVE-2014-9427	128.122.128.69	80	11/10/2019, 11:04:18 AM	1/2/2015, 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-2016-1908	128.122.93.210	22	11/6/2019, 10:55:05 PM	4/11/2017, 12:00:00 AM
Vulnerability Description : The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.				
CVE-2016-6515	128.122.93.210	22	11/6/2019, 10:55:05 PM	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-2014-3515	128.238.182.18	80	10/19/2019, 5:33:28 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPObjectStorage.				
CVE-2014-3669	128.238.182.18	80	10/19/2019, 5:33:28 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.238.182.18	80	10/19/2019, 5:33:28 PM	1/2/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2014-9427	128.122.4.236	443	10/16/2019, 4:53:03 AM	1/2/2015, 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-2014-3669	128.122.4.236	443	10/16/2019, 4:53:03 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.4.236	443	10/16/2019, 4:53:03 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.4.236	80	10/11/2019, 2:57:57 AM	1/2/2015, 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-2014-3515	128.122.4.236	80	10/11/2019, 2:57:57 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.130.129	80	10/11/2019, 1:32:22 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.130.129	80	10/11/2019, 1:32:22 AM	1/2/2015, 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-2006-0058	128.122.128.10	25	10/8/2019, 10:54:11 AM	3/22/2006, 12:00:00 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2009-4565	128.122.128.10	25	10/8/2019, 10:54:11 AM	1/4/2010, 12:00:00 AM

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2003-0161	128.122.112.176	25	10/7/2019, 11:44:27 PM	4/2/2003, 12:00:00 AM
Vulnerability Description : The prescan() function in the address parser (parseaddr.c) in Sendmail before 8.12.9 does not properly handle certain conversions from char and int types, which can cause a length check to be disabled when Sendmail misinterprets an input value as a special "NOCHAR" control value, allowing attackers to cause a denial of service and possibly execute arbitrary code via a buffer overflow attack using messages, a different vulnerability than CVE-2002-1337.				
CVE-2009-4565	128.122.112.176	25	10/7/2019, 11:44:27 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2002-0906	128.122.112.176	25	10/7/2019, 11:44:27 PM	10/4/2002, 12:00:00 AM
Vulnerability Description : Buffer overflow in Sendmail before 8.12.5, when configured to use a custom DNS map to query TXT records, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a malicious DNS server.				
CVE-2002-2261	128.122.112.176	25	10/7/2019, 11:44:27 PM	12/31/2002, 12:00:00 AM
Vulnerability Description : Sendmail 8.9.0 through 8.12.6 allows remote attackers to bypass relaying restrictions enforced by the 'check_relay' function by spoofing a blank DNS hostname.				
CVE-2002-1337	128.122.112.176	25	10/7/2019, 11:44:27 PM	3/7/2003, 12:00:00 AM
Vulnerability Description : Buffer overflow in Sendmail 5.7.9 to 8.12.7 allows remote attackers to execute arbitrary code via certain formatted address fields, related to sender and recipient header comments as processed by the crackaddr function of headers.c.				
CVE-2014-9427	128.238.182.18	443	10/2/2019, 10:37:16 AM	1/2/2015, 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-2009-4565	216.165.47.33	465	9/16/2019, 5:03:37 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2014-9427	216.165.26.109	443	9/14/2019, 4:07:18 PM	1/2/2015, 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-2014-3515	216.165.26.109	443	9/14/2019, 4:07:18 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	216.165.26.109	443	9/14/2019, 4:07:18 PM	10/29/2014, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.108.67	80	9/11/2019, 1:00:07 AM	1/2/2015, 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-2014-8626	128.122.108.67	80	9/11/2019, 1:00:07 AM	11/22/2014, 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-2011-3268	128.122.108.68	80	9/11/2019, 12:54:49 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-2014-9427	128.122.108.68	80	9/11/2019, 12:54:49 AM	1/2/2015, 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-2014-8626	128.122.108.68	80	9/11/2019, 12:54:49 AM	11/22/2014, 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-2014-9427	128.122.2.44	80	9/10/2019, 5:05:08 PM	1/2/2015, 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-2011-3268	128.122.108.66	80	9/10/2019, 2:24:17 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-2014-8626	128.122.108.66	80	9/10/2019, 2:24:17 AM	11/22/2014, 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-2014-9427	128.122.108.66	80	9/10/2019, 2:24:17 AM	1/2/2015, 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-2014-9427	128.122.108.88	80	9/10/2019, 2:21:11 AM	1/2/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2014-8626	128.122.108.88	80	9/10/2019, 2:21:11 AM	11/22/2014, 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-2014-9427	128.122.114.12	80	9/9/2019, 11:19:35 AM	1/2/2015, 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-2014-9427	128.238.63.50	443	8/16/2019, 10:52:24 AM	1/2/2015, 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-2011-3268	128.238.63.50	443	8/16/2019, 10:52:24 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-2014-8626	128.238.63.35	443	8/14/2019, 5:21:12 PM	11/22/2014, 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-2011-3268	128.238.63.35	443	8/14/2019, 5:21:12 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-2014-9427	128.238.63.35	443	8/14/2019, 5:21:12 PM	1/2/2015, 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-2014-8626	128.238.63.35	80	8/13/2019, 4:51:25 AM	11/22/2014, 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-2014-9427	128.238.63.35	80	8/13/2019, 4:51:25 AM	1/2/2015, 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-2011-3268	128.238.63.35	80	8/13/2019, 4:51:25 AM	8/25/2011, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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	128.238.63.50	80	8/12/2019, 4:29:19 PM	11/22/2014, 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-2011-3268	128.238.63.50	80	8/12/2019, 4:29:19 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-2014-9427	128.238.63.50	80	8/12/2019, 4:29:19 PM	1/2/2015, 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-2014-9427	128.122.128.34	80	8/10/2019, 10:31:12 AM	1/2/2015, 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-2016-10009	128.122.97.248	22	8/7/2019, 11:58:13 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	128.122.97.248	22	8/7/2019, 11:58:13 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 allow 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	128.122.97.238	22	8/7/2019, 11:51:25 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	128.122.97.238	22	8/7/2019, 11:51:25 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 allow 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-2016-10012	128.122.95.63	22	8/7/2019, 7:15:37 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 allow 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	128.122.95.63	22	8/7/2019, 7:15:37 AM	1/4/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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	128.122.250.27	22	8/7/2019, 4:36:46 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	128.122.97.242	22	8/6/2019, 10:15:45 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.				
CVE-2016-10012	128.122.97.242	22	8/6/2019, 10:15:45 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 allow 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-2014-3669	128.122.4.13	443	7/20/2019, 12:26:00 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.115.153	80	7/14/2019, 4:13:19 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.122.115.153	80	7/14/2019, 4:13:19 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.115.153	80	7/14/2019, 4:13:19 PM	1/2/2015, 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-2017-9078	128.122.227.241	22	7/12/2019, 9:24:03 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-2016-10009	128.122.97.245	22	7/12/2019, 4:50:12 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	128.122.97.245	22	7/12/2019, 4:50:12 AM	1/4/2017, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
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 allow 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-2014-3515	128.238.182.18	443	6/14/2019, 11:41:56 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3669	128.238.182.18	443	6/14/2019, 11:41:56 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.238.66.15	443	6/13/2019, 9:37:44 PM	1/2/2015, 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-2014-9427	128.238.66.15	80	6/9/2019, 2:17:07 AM	1/2/2015, 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-2014-9427	128.122.86.187	80	6/8/2019, 9:27:45 PM	1/2/2015, 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-2009-4565	128.238.66.13	25	6/8/2019, 12:17:16 AM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a "\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2017-7668	18.179.160.39	80	6/4/2019, 1:21:53 AM	6/19/2017, 12:00:00 AM
Vulnerability Description : The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.				
CVE-2017-7668	18.179.160.39	443	5/23/2019, 8:47:41 AM	6/19/2017, 12:00:00 AM
Vulnerability Description : The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.				
CVE-2015-3329	216.165.125.109	443	5/11/2019, 6:05:42 AM	6/9/2015, 12:00:00 AM
Vulnerability Description : Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-9705	216.165.125.109	443	5/11/2019, 6:05:42 AM	3/30/2015, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2015-3307	216.165.125.109	443	5/11/2019, 6:05:42 AM	6/9/2015, 12:00:00 AM
Vulnerability Description : The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.				
CVE-2015-4022	216.165.125.109	443	5/11/2019, 6:05:42 AM	6/9/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.				
CVE-2014-3669	128.122.130.72	80	5/8/2019, 11:29:17 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.238.66.13	80	5/8/2019, 4:25:52 AM	1/2/2015, 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-2006-0058	128.122.128.77	25	5/6/2019, 6:36:33 PM	3/22/2006, 12:00:00 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2009-4565	128.122.128.78	25	5/6/2019, 6:33:17 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2009-4565	128.122.128.37	25	5/6/2019, 1:39:53 PM	1/4/2010, 12:00:00 AM
Vulnerability Description : sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.				
CVE-2006-0058	128.122.128.37	25	5/6/2019, 1:39:53 PM	3/22/2006, 12:00:00 AM
Vulnerability Description : Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggering timeouts in a way that causes the setjmp and longjmp function calls to be interrupted and modify unexpected memory locations.				
CVE-2014-9427	128.122.85.21	443	4/19/2019, 8:00:52 AM	1/2/2015, 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-2014-3669	128.122.108.145	443	4/19/2019, 7:45:21 AM	10/29/2014, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.108.145	443	4/19/2019, 7:45:21 AM	1/2/2015, 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-2014-3515	128.122.108.145	443	4/19/2019, 7:45:21 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2015-2331	216.165.127.109	443	4/19/2019, 1:41:47 AM	3/30/2015, 12:00:00 AM
Vulnerability Description : Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.				
CVE-2014-9705	216.165.127.109	443	4/19/2019, 1:41:47 AM	3/30/2015, 12:00:00 AM
Vulnerability Description : Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2014-9427	128.122.49.123	443	4/17/2019, 9:16:22 PM	1/2/2015, 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-2014-3669	128.122.49.123	443	4/17/2019, 9:16:22 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.123	443	4/17/2019, 9:16:22 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.85.21	80	4/14/2019, 11:18:47 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.108.145	80	4/14/2019, 11:02:31 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2014-9427	128.122.108.145	80	4/14/2019, 11:02:31 PM	1/2/2015, 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-2014-3669	128.122.108.145	80	4/14/2019, 11:02:31 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.8.38	80	4/14/2019, 1:48:24 PM	1/2/2015, 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-2014-3669	128.122.8.38	80	4/14/2019, 1:48:24 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.8.38	80	4/14/2019, 1:48:24 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.128.72	80	4/14/2019, 9:47:08 AM	1/2/2015, 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-2014-3669	128.122.49.27	80	4/13/2019, 9:54:49 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.49.27	80	4/13/2019, 9:54:49 PM	1/2/2015, 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-2014-3515	128.122.49.27	80	4/13/2019, 9:54:49 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9705	216.165.26.240	80	4/13/2019, 7:38:49 PM	3/30/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
Vulnerability Description : Heap-based buffer overflow in the <code>enchant_broker_request_dict</code> function in <code>ext/enchant/enchant.c</code> in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.				
CVE-2015-4026	216.165.26.240	80	4/13/2019, 7:38:49 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The <code>pcntl_exec</code> implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a <code>\x00</code> character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.				
CVE-2015-2301	216.165.26.240	80	4/13/2019, 7:38:49 PM	3/30/2015, 12:00:00 AM
Vulnerability Description : Use-after-free vulnerability in the <code>phar_rename_archive</code> function in <code>phar_object.c</code> in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.				
CVE-2015-3307	216.165.26.240	80	4/13/2019, 7:38:49 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : The <code>phar_parse_metadata</code> function in <code>ext/phar/phar.c</code> in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.				
CVE-2015-3329	216.165.26.240	80	4/13/2019, 7:38:49 PM	6/9/2015, 12:00:00 AM
Vulnerability Description : Multiple stack-based buffer overflows in the <code>phar_set_inode</code> function in <code>phar_internal.h</code> in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.				
CVE-2014-3669	128.122.49.123	80	4/13/2019, 7:22:03 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the <code>object_custom</code> function in <code>ext/standard/var_unserializer.c</code> in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the <code>unserialize</code> function that triggers calculation of a large length value.				
CVE-2014-3515	128.122.49.123	80	4/13/2019, 7:22:03 AM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) <code>ArrayObject</code> and (2) <code>SPLObjectStorage</code> .				
CVE-2014-9427	128.122.49.123	80	4/13/2019, 7:22:03 AM	1/2/2015, 12:00:00 AM
Vulnerability Description : <code>sapi/cgi/cgi_main.c</code> 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 <code>mmap</code> 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-2011-3268	128.122.108.67	80	4/13/2019, 5:45:38 AM	8/25/2011, 12:00:00 AM
Vulnerability Description : Buffer overflow in the <code>crypt</code> 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-2014-3669	128.122.4.236	80	4/13/2019, 5:08:56 AM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the <code>object_custom</code> function in <code>ext/standard/var_unserializer.c</code> in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the <code>unserialize</code> function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.128.25	80	4/13/2019, 4:36:28 AM	1/2/2015, 12:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2014-3669	128.122.4.13	80	4/12/2019, 8:23:08 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				
CVE-2014-9427	128.122.4.13	80	4/12/2019, 8:23:08 PM	1/2/2015, 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-2014-3515	128.122.4.13	80	4/12/2019, 8:23:08 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-3515	128.122.4.48	80	4/12/2019, 6:56:26 PM	7/9/2014, 12:00:00 AM
Vulnerability Description : The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.				
CVE-2014-9427	128.122.4.48	80	4/12/2019, 6:56:26 PM	1/2/2015, 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-2014-3669	128.122.4.48	80	4/12/2019, 6:56:26 PM	10/29/2014, 12:00:00 AM
Vulnerability Description : Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.				

## ! Low Severity CVEs Patching Cadence

-0.2 SCORE IMPACT

Low severity vulnerability seen network more than 180 days after CVE was published.

### Description

Based on scan data, the company had low severity CVE vulnerability that was open longer than 180 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 180 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 BugTraq mailing list 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.

## 6 findings

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	LAST OBSERVED OPEN	VULNERABILITY PUBLISH DATE
CVE-2016-10011	128.122.250.36	22	1/5/2020, 4:24:57 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-2014-3956	128.238.66.55	25	12/10/2019, 12:12:33 PM	6/4/2014, 12:00:00 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.60.87	25	10/8/2019, 5:59:08 AM	6/4/2014, 12:00:00 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2002-1827	128.122.112.176	25	10/7/2019, 11:44:27 PM	12/31/2002, 12:00:00 AM
Vulnerability Description : Sendmail 8.9.0 through 8.12.3 allows local users to cause a denial of service by obtaining an exclusive lock on the (1) alias, (2) map, (3) statistics, and (4) pid files.				
CVE-2014-3956	216.165.47.32	25	10/7/2019, 11:39:17 PM	6/4/2014, 12:00:00 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				
CVE-2014-3956	128.122.49.17	25	10/7/2019, 8:58:03 PM	6/4/2014, 12:00:00 AM
Vulnerability Description : The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.				

## !! End-of-Life Product

-<0.1 SCORE IMPACT

We observed an end-of-life product, one that is no longer developed or sold, publicly exposed.

### Description

A product that has been declared as end-of-life (EOL) by the manufacturer has been detected. An EOL product is no longer marketed, sold, or upgraded by the manufacturer. Products at this stage in their life cycle are more likely to have vulnerabilities that will remain unpatched.

### Recommendation

Ensure the affected product has an extended support contract that includes security patches. Review the vendor's statement of EOL guidelines for replacement products and upgrade to a new product line or manufacturer.

1 finding

PRODUCT VERSION	IP ADDRESS	PORT	END OF LIFE DATE	PRODUCT MANUFACTURER	PRODUCT NAME	MANUFACTURER STATEMENT	LAST OBSERVED
7.0	128.122.83.195	80	1/13/2015, 12:00:00 AM	Microsoft	Internet Information Services 7.0	<a href="https://support.microsoft.com/en-us/lifecycle?p1=12925">https://support.microsoft.com/en-us/lifecycle?p1=12925</a>	2/7/2020, 5:23:14 AM

## !! Medium-Severity Vulnerability in Last Observation

-0.8 SCORE IMPACT

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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-2006-1173	128.122.128.10	587	6/7/2006, 12:00:00 AM	3/11/2020, 7:34:22 PM
Vulnerability Description : Sendmail before 8.13.7 allows remote attackers to cause a denial of service via deeply nested, malformed multipart MIME messages that exhaust the stack during the recursive mime8to7 function for performing 8-bit to 7-bit conversion, which prevents Sendmail from delivering queued messages and might lead to disk consumption by core dump files.				
CVE-2006-4434	128.122.128.10	587	8/28/2008, 12:00:00 AM	3/11/2020, 7:34:22 PM
Vulnerability Description : Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is unlikely)... the bug is in the shutdown code (finis()) which leads directly to exit(3), i.e., the process would terminate anyway, no mail delivery or reception is affected."				
CVE-2006-4434	193.175.54.5	587	8/28/2008, 12:00:00 AM	3/11/2020, 6:08:12 PM
Vulnerability Description : Use-after-free vulnerability in Sendmail before 8.13.8 allows remote attackers to cause a denial of service (crash) via a long "header line", which causes a previously freed variable to be referenced. NOTE: the original developer has disputed the severity of this issue, saying "The only denial of service that is possible here is to fill up the disk with core dumps if the OS actually generates different core dumps (which is unlikely)... the bug is in the shutdown code (finis()) which leads directly to exit(3), i.e., the process would terminate anyway, no mail delivery or reception is affected."				
CVE-2006-1173	193.175.54.5	587	6/7/2006, 12:00:00 AM	3/11/2020, 6:08:12 PM
Vulnerability Description : Sendmail before 8.13.7 allows remote attackers to cause a denial of service via deeply nested, malformed multipart MIME messages that exhaust the stack during the recursive mime8to7 function for performing 8-bit to 7-bit conversion, which prevents Sendmail from delivering queued messages and might lead to disk consumption by core dump files.				
CVE-2016-8743	128.122.130.31	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:50:24 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-2016-8743	128.122.130.6	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:12:15 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-2016-8743	128.122.130.73	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:02:57 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8743	128.122.108.134	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:02:48 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-2016-8743	128.122.108.133	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:02:06 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-2016-8743	128.238.63.20	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:01:34 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-2017-7529	128.238.63.21	443	7/13/2017, 12:00:00 AM	3/10/2020, 11:00:13 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-2016-8743	128.122.108.161	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:59:20 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-2016-8743	128.122.108.130	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:57:29 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-2015-3197	128.122.108.130	443	2/14/2016, 12:00:00 AM	3/10/2020, 10:57:29 PM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2015-3195	128.122.108.130	443	12/6/2015, 12:00:00 AM	3/10/2020, 10:57:29 PM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2015-3194	128.122.108.130	443	12/6/2015, 12:00:00 AM	3/10/2020, 10:57:29 PM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2016-8743	128.122.108.143	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:55:02 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-2016-8743	128.122.108.64	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:54:40 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-3738	128.122.108.128	443	12/7/2017, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.108.128	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.108.128	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:53:26 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-2017-3736	128.122.108.128	443	11/2/2017, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	128.122.108.128	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	128.122.108.128	443	12/7/2017, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	128.122.108.128	443	7/20/2014, 12:00:00 AM	3/10/2020, 10:53:26 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.108.82	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:52:43 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2015-3185	128.122.108.82	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:52:43 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.108.82	443	7/20/2014, 12:00:00 AM	3/10/2020, 10:52:43 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.108.82	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:52:43 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.108.22	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:52:32 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-2016-8743	128.122.108.121	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:52:11 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-2016-8743	128.122.108.12	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:52:08 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-2016-8743	128.122.108.59	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:51:45 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-2016-8743	216.165.85.216	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:28:13 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-2015-3185	216.165.85.216	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:28:13 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	216.165.85.216	443	7/20/2015, 12:00:00 AM	3/10/2020, 10:28:13 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, (1) ANYWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, (2) ACCURACY, RESULTS, TIMELINESS AND COMPLETENESS, (3) FREEDOM FROM BUGS, SOFTWARE ERRORS AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	216.165.85.216	443	7/20/2014, 12:00:00 AM	3/10/2020, 10:28:13 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-7529	3.234.69.139	443	7/13/2017, 12:00:00 AM	3/10/2020, 9:59:46 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-2016-8743	34.213.36.80	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:42:51 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-2015-3185	91.230.41.15	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:05:26 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	91.230.41.15	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:05:26 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-2015-3183	91.230.41.15	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:05:26 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	91.230.41.15	443	7/20/2014, 12:00:00 AM	3/10/2020, 9:05:26 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-7529	128.122.180.64	443	7/13/2017, 12:00:00 AM	3/10/2020, 8:56:02 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-2017-7529	128.122.90.72	443	7/13/2017, 12:00:00 AM	3/10/2020, 8:19:42 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-2016-4450	128.122.90.72	443	6/7/2016, 12:00:00 AM	3/10/2020, 8:19:42 PM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2017-3736	34.207.146.41	443	11/2/2017, 12:00:00 AM	3/10/2020, 7:49:23 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	34.207.146.41	443	12/7/2017, 12:00:00 AM	3/10/2020, 7:49:23 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	34.207.146.41	443	12/7/2017, 12:00:00 AM	3/10/2020, 7:49:23 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	216.165.32.96	443	7/27/2017, 12:00:00 AM	3/10/2020, 7:24:45 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-2017-7529	128.122.228.13	443	7/13/2017, 12:00:00 AM	3/10/2020, 6:26:48 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-2016-4450	128.122.228.13	443	6/7/2016, 12:00:00 AM	3/10/2020, 6:26:48 PM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2017-7529	128.122.59.145	443	7/13/2017, 12:00:00 AM	3/10/2020, 5:52:47 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-2016-4450	128.122.59.145	443	6/7/2016, 12:00:00 AM	3/10/2020, 5:52:47 PM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-8743	128.122.149.60	443	7/27/2017, 12:00:00 AM	3/10/2020, 5:46:06 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2015-3183	216.165.26.240	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	216.165.26.240	443	12/7/2017, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	216.165.26.240	443	12/7/2017, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	216.165.26.240	443	7/20/2014, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	216.165.26.240	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:28:24 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-2015-3185	216.165.26.240	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	216.165.26.240	443	11/2/2017, 12:00:00 AM	3/10/2020, 4:28:24 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-3566	128.122.65.146	8443	10/14/2014, 12:00:00 AM	3/10/2020, 3:25:20 PM
Vulnerability Description : The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.				
CVE-2014-0226	128.122.49.71	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:31:06 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	128.122.49.71	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:31:06 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	128.122.49.71	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:31:06 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.49.71	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:31:06 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.122.49.71	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:31:06 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.49.71	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:31:06 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-2017-3737	128.122.49.71	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:31:06 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	128.122.49.52	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:25:32 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-0226	128.122.49.52	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:25:32 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.49.52	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:25:32 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-2017-3737	128.122.49.52	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:25:32 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	128.122.49.52	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:25:32 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.49.52	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:25:32 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	128.122.49.52	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:25:32 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.108	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:37 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.49.108	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:22:37 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-2014-0226	128.122.49.108	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:22:37 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.122.49.108	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:37 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.49.108	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:37 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.49.108	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:37 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.49.108	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:22:37 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	128.122.49.28	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.28	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3736	128.122.49.28	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.49.28	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:22:21 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-3737	128.122.49.28	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2017-3738	128.122.49.28	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 11.0 at this time. The fix will be included in OpenSSL 11.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.49.28	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:21 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3737	128.122.49.98	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:18 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2017-3736	128.122.49.98	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:22:18 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.49.98	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:18 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.49.98	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:22:18 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.49.98	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:22:18 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.49.98	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:22:18 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-2015-3185	128.122.49.98	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:22:18 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-3597	128.122.49.75	443	8/22/2014, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2017-3736	128.122.49.75	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.49.75	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.122.49.75	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:16:45 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-2015-0232	128.122.49.75	443	1/27/2015, 12:00:00 AM	3/10/2020, 2:16:45 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-3670	128.122.49.75	443	10/29/2014, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2015-3183	128.122.49.75	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.49.75	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.75	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3737	128.122.49.75	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:16:45 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	128.122.49.59	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.49.59	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.122.49.59	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:16:43 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2015-3183	128.122.49.59	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3737	128.122.49.59	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.122.49.59	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.59	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:16:43 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	128.122.49.17	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	128.122.49.17	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 11.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-0232	128.122.49.17	443	1/27/2015, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2015-3183	128.122.49.17	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.49.17	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:15:38 PM
Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2014-3597	128.122.49.17	443	8/22/2014, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2017-3737	128.122.49.17	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	128.122.49.17	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-0226	128.122.49.17	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3670	128.122.49.17	443	10/29/2014, 12:00:00 AM	3/10/2020, 2:15:38 PM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2014-0226	128.122.49.48	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:14:58 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.49.114	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:14:58 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-2017-3737	128.122.49.48	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:14:58 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.49.48	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:14:58 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-2017-3736	128.122.49.48	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:14:58 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.49.48	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:14:58 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.49.48	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:14:58 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	128.122.49.48	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:14:58 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	216.165.47.13	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	216.165.47.13	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8743	216.165.47.13	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:11:18 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-2014-0226	216.165.47.13	443	7/20/2014, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	216.165.47.13	443	12/7/2017, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	216.165.47.13	443	11/2/2017, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	216.165.47.13	443	7/20/2015, 12:00:00 AM	3/10/2020, 2:11:18 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	3.225.114.16	443	12/7/2017, 12:00:00 AM	3/10/2020, 1:36:38 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	3.225.114.16	443	11/2/2017, 12:00:00 AM	3/10/2020, 1:36:38 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	3.225.114.16	443	12/7/2017, 12:00:00 AM	3/10/2020, 1:36:38 PM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-0703	128.122.108.158	443	3/2/2016, 12:00:00 AM	3/10/2020, 12:04:00 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-2016-8743	128.122.108.158	443	7/27/2017, 12:00:00 AM	3/10/2020, 12:04:00 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-2015-3195	128.122.108.158	443	12/6/2015, 12:00:00 AM	3/10/2020, 12:04:00 PM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2014-0226	128.122.120.72	443	7/20/2014, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3670	128.122.120.72	443	10/29/2014, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3737	128.122.120.72	443	12/7/2017, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-3597	128.122.120.72	443	8/22/2014, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-0232	128.122.120.72	443	1/27/2015, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2015-3183	128.122.120.72	443	7/20/2015, 12:00:00 AM	3/10/2020, 11:58:17 AM
Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.122.120.72	443	7/20/2015, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	128.122.120.72	443	12/7/2017, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	128.122.120.72	443	11/2/2017, 12:00:00 AM	3/10/2020, 11:58:17 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.120.72	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:58:17 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-2017-3736	34.196.167.182	443	11/2/2017, 12:00:00 AM	3/10/2020, 11:46:57 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	34.196.167.182	443	12/7/2017, 12:00:00 AM	3/10/2020, 11:46:57 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3738	34.196.167.182	443	12/7/2017, 12:00:00 AM	3/10/2020, 11:46:57 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.238.66.55	443	7/27/2017, 12:00:00 AM	3/10/2020, 11:29:05 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-2016-0703	128.238.66.55	443	3/2/2016, 12:00:00 AM	3/10/2020, 11:29:05 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-2016-8743	216.165.32.97	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:54:27 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-2016-8743	128.122.112.30	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:39:53 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-2016-0703	128.122.112.30	443	3/2/2016, 12:00:00 AM	3/10/2020, 10:39:53 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-2016-8743	128.122.4.30	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:34:47 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-2016-8743	128.122.112.23	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:32:58 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-2016-8743	91.230.41.37	443	7/27/2017, 12:00:00 AM	3/10/2020, 10:25:45 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	91.230.41.43	443	7/13/2017, 12:00:00 AM	3/10/2020, 10:22:07 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-7529	91.230.41.25	443	7/13/2017, 12:00:00 AM	3/10/2020, 10:17:00 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-2016-8743	128.122.114.42	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:50:35 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-2016-0703	128.122.114.42	443	3/2/2016, 12:00:00 AM	3/10/2020, 9:50:35 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-2014-0226	128.122.4.12	443	7/20/2014, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.122.4.12	443	12/7/2017, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	128.122.4.12	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	128.122.4.12	443	12/7/2017, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.4.12	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:49:39 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-2015-0232	128.122.4.12	443	1/27/2015, 12:00:00 AM	3/10/2020, 9:49:39 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3736	128.122.4.12	443	11/2/2017, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-3670	128.122.4.12	443	10/29/2014, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2015-3183	128.122.4.12	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3597	128.122.4.12	443	8/22/2014, 12:00:00 AM	3/10/2020, 9:49:39 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2016-8743	128.122.128.72	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:42:02 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-2016-0703	128.122.128.72	443	3/2/2016, 12:00:00 AM	3/10/2020, 9:42:02 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-2016-8743	128.122.4.44	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:41:19 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-2016-0703	128.122.128.25	443	3/2/2016, 12:00:00 AM	3/10/2020, 9:39:23 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-2016-8743	128.122.128.25	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:39:23 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8743	128.122.128.45	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:33:01 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-2016-0703	128.122.128.45	443	3/2/2016, 12:00:00 AM	3/10/2020, 9:33:01 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-2015-3183	128.122.4.238	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:24:57 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	128.122.4.238	443	7/20/2014, 12:00:00 AM	3/10/2020, 9:24:57 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	128.122.4.238	443	7/20/2015, 12:00:00 AM	3/10/2020, 9:24:57 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.4.238	443	7/27/2017, 12:00:00 AM	3/10/2020, 9:24:57 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-2017-3738	128.238.26.32	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.238.26.32	80	7/20/2014, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-0232	128.238.26.32	80	1/27/2015, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3737	128.238.26.32	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:51:15 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-3597	128.238.26.32	80	8/22/2014, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2016-8743	128.238.26.32	80	7/27/2017, 12:00:00 AM	3/10/2020, 8:51:15 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-2017-3736	128.238.26.32	80	11/2/2017, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-3670	128.238.26.32	80	10/29/2014, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2015-3185	128.238.26.32	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.238.26.32	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:51:15 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	52.1.126.186	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:37:31 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-2014-0226	91.230.41.217	443	7/20/2014, 12:00:00 AM	3/10/2020, 8:37:30 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	91.230.41.217	443	7/20/2015, 12:00:00 AM	3/10/2020, 8:37:30 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	91.230.41.217	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:37:30 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-2015-3185	91.230.41.217	443	7/20/2015, 12:00:00 AM	3/10/2020, 8:37:30 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-0703	180.169.77.47	443	3/2/2016, 12:00:00 AM	3/10/2020, 8:27:00 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-2015-3195	180.169.77.47	443	12/6/2015, 12:00:00 AM	3/10/2020, 8:27:00 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2015-3194	180.169.77.47	443	12/6/2015, 12:00:00 AM	3/10/2020, 8:27:00 AM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2016-8743	180.169.77.47	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:27:00 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-2015-3197	180.169.77.47	443	2/14/2016, 12:00:00 AM	3/10/2020, 8:27:00 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2016-8743	128.238.182.100	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:22:40 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-2016-8743	128.122.4.26	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:19:07 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-2015-3183	18.234.142.204	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:18:04 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	18.234.142.204	80	11/2/2017, 12:00:00 AM	3/10/2020, 8:18:04 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	18.234.142.204	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:18:04 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-10.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 11.0 at this time. The fix will be included in OpenSSL 11.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	18.234.142.204	80	7/20/2014, 12:00:00 AM	3/10/2020, 8:18:04 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	18.234.142.204	80	7/27/2017, 12:00:00 AM	3/10/2020, 8:18:04 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-2015-3185	18.234.142.204	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:18:04 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	18.234.142.204	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:18:04 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.4.45	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:15:38 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	34.193.12.206	443	7/13/2017, 12:00:00 AM	3/10/2020, 8:14:14 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-7529	128.238.66.230	80	7/13/2017, 12:00:00 AM	3/10/2020, 8:07:27 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-2015-3183	216.165.49.28	443	7/20/2015, 12:00:00 AM	3/10/2020, 8:04:55 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	216.165.49.28	443	7/20/2015, 12:00:00 AM	3/10/2020, 8:04:55 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	216.165.49.28	443	7/27/2017, 12:00:00 AM	3/10/2020, 8:04:55 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-2014-0226	216.165.49.28	443	7/20/2014, 12:00:00 AM	3/10/2020, 8:04:55 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	66.228.45.202	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:02:17 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	66.228.45.202	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:02:17 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	66.228.45.202	80	11/2/2017, 12:00:00 AM	3/10/2020, 8:02:17 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	66.228.45.202	80	12/7/2017, 12:00:00 AM	3/10/2020, 8:02:17 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	66.228.45.202	80	7/20/2015, 12:00:00 AM	3/10/2020, 8:02:17 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	66.228.45.202	80	7/20/2014, 12:00:00 AM	3/10/2020, 8:02:17 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	66.228.45.202	80	7/27/2017, 12:00:00 AM	3/10/2020, 8:02:17 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-2014-0226	128.238.63.87	80	7/20/2014, 12:00:00 AM	3/10/2020, 7:38:00 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.238.63.87	80	7/27/2017, 12:00:00 AM	3/10/2020, 7:38:00 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-2017-3737	128.238.63.87	80	12/7/2017, 12:00:00 AM	3/10/2020, 7:38:00 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	128.238.63.87	80	11/2/2017, 12:00:00 AM	3/10/2020, 7:38:00 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.238.63.87	80	7/20/2015, 12:00:00 AM	3/10/2020, 7:38:00 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.238.63.87	80	7/20/2015, 12:00:00 AM	3/10/2020, 7:38:00 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	128.238.63.87	80	12/7/2017, 12:00:00 AM	3/10/2020, 7:38:00 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-7529	128.238.66.155	443	7/13/2017, 12:00:00 AM	3/10/2020, 7:36:14 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-2016-8743	128.122.60.87	443	7/27/2017, 12:00:00 AM	3/10/2020, 7:35:49 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-2017-7529	128.238.66.235	443	7/13/2017, 12:00:00 AM	3/10/2020, 7:31:54 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-2017-7529	128.238.66.230	443	7/13/2017, 12:00:00 AM	3/10/2020, 7:27:19 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-2016-8743	52.0.197.6	80	7/27/2017, 12:00:00 AM	3/10/2020, 7:08:57 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-2016-8743	66.35.39.41	80	7/27/2017, 12:00:00 AM	3/10/2020, 6:48:00 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-2016-8743	128.122.108.91	443	7/27/2017, 12:00:00 AM	3/10/2020, 6:44:41 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8743	128.122.108.13	443	7/27/2017, 12:00:00 AM	3/10/2020, 6:44:22 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-2016-8743	128.122.108.23	443	7/27/2017, 12:00:00 AM	3/10/2020, 6:40:54 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-2015-3183	128.122.108.60	443	7/20/2015, 12:00:00 AM	3/10/2020, 6:36:38 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.108.60	443	7/27/2017, 12:00:00 AM	3/10/2020, 6:36:38 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-2014-0226	128.122.108.60	443	7/20/2014, 12:00:00 AM	3/10/2020, 6:36:38 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	128.122.108.60	443	7/20/2015, 12:00:00 AM	3/10/2020, 6:36:38 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	34.207.146.41	80	12/7/2017, 12:00:00 AM	3/10/2020, 6:36:36 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	34.207.146.41	80	11/2/2017, 12:00:00 AM	3/10/2020, 6:36:36 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	34.207.146.41	80	12/7/2017, 12:00:00 AM	3/10/2020, 6:36:36 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	34.214.227.165	443	7/27/2017, 12:00:00 AM	3/10/2020, 6:17:59 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-2016-8743	91.230.41.44	80	7/27/2017, 12:00:00 AM	3/10/2020, 6:05:27 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-2014-0226	52.1.187.2	443	7/20/2014, 12:00:00 AM	3/10/2020, 5:45:41 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3185	52.1.187.2	443	7/20/2015, 12:00:00 AM	3/10/2020, 5:45:41 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	52.1.187.2	443	7/27/2017, 12:00:00 AM	3/10/2020, 5:45:41 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-2017-3737	52.1.187.2	443	12/7/2017, 12:00:00 AM	3/10/2020, 5:45:41 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	52.1.187.2	443	7/20/2015, 12:00:00 AM	3/10/2020, 5:45:41 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	52.1.187.2	443	11/2/2017, 12:00:00 AM	3/10/2020, 5:45:41 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	52.1.187.2	443	12/7/2017, 12:00:00 AM	3/10/2020, 5:45:41 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.238.182.21	80	7/27/2017, 12:00:00 AM	3/10/2020, 5:44:46 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	128.122.136.123	443	7/13/2017, 12:00:00 AM	3/10/2020, 5:15:42 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-2016-8743	128.238.63.17	80	7/27/2017, 12:00:00 AM	3/10/2020, 5:12:32 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-2017-3738	34.231.72.14	443	12/7/2017, 12:00:00 AM	3/10/2020, 5:08:21 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	34.231.72.14	443	12/7/2017, 12:00:00 AM	3/10/2020, 5:08:21 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	34.231.72.14	443	11/2/2017, 12:00:00 AM	3/10/2020, 5:08:21 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-7529	128.238.147.221	80	7/13/2017, 12:00:00 AM	3/10/2020, 5:06:23 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-2015-3194	128.122.238.249	443	12/6/2015, 12:00:00 AM	3/10/2020, 5:04:41 AM
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2016-8743	128.122.238.249	443	7/27/2017, 12:00:00 AM	3/10/2020, 5:04:41 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-2015-3195	128.122.238.249	443	12/6/2015, 12:00:00 AM	3/10/2020, 5:04:41 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2015-3197	128.122.238.249	443	2/14/2016, 12:00:00 AM	3/10/2020, 5:04:41 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2016-0703	128.122.238.249	443	3/2/2016, 12:00:00 AM	3/10/2020, 5:04:41 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-2015-3185	59.79.127.150	80	7/20/2015, 12:00:00 AM	3/10/2020, 4:58:27 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	59.79.127.150	80	7/27/2017, 12:00:00 AM	3/10/2020, 4:58:27 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-2015-3183	59.79.127.150	80	7/20/2015, 12:00:00 AM	3/10/2020, 4:58:27 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	59.79.127.150	80	7/20/2014, 12:00:00 AM	3/10/2020, 4:58:27 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-2783	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.				
CVE-2015-4024	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/fc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.				
CVE-2015-0232	128.238.63.75	443	1/27/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-0226	128.238.63.75	443	7/20/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.238.63.75	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:42:31 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-2015-3185	128.238.63.75	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-9652	128.238.63.75	443	3/30/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.				
CVE-2015-3330	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."				
CVE-2015-4021	128.238.63.75	443	6/9/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the 0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.				
CVE-2015-3194	128.238.63.75	443	12/6/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.				
CVE-2015-3195	128.238.63.75	443	12/6/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.				
CVE-2015-3183	128.238.63.75	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3597	128.238.63.75	443	8/22/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-3197	128.238.63.75	443	2/14/2016, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.				
CVE-2016-0703	128.238.63.75	443	3/2/2016, 12:00:00 AM	3/10/2020, 4:42:31 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-2014-3670	128.238.63.75	443	10/29/2014, 12:00:00 AM	3/10/2020, 4:42:31 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2016-8743	128.238.63.28	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:40:55 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-2014-0226	128.238.63.88	443	7/20/2014, 12:00:00 AM	3/10/2020, 4:40:03 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.238.63.88	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:40:03 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-2015-3185	128.238.63.88	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:40:03 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	128.238.63.88	443	12/7/2017, 12:00:00 AM	3/10/2020, 4:40:03 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3738	128.238.63.88	443	12/7/2017, 12:00:00 AM	3/10/2020, 4:40:03 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.238.63.88	443	7/20/2015, 12:00:00 AM	3/10/2020, 4:40:03 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.238.63.88	443	11/2/2017, 12:00:00 AM	3/10/2020, 4:40:03 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	216.165.47.56	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:35:31 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-2016-8743	128.238.66.89	80	7/27/2017, 12:00:00 AM	3/10/2020, 4:32:52 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-2016-8743	128.238.63.22	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:32:20 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	3.234.69.139	80	7/13/2017, 12:00:00 AM	3/10/2020, 4:25:09 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2016-8743	128.238.63.13	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:19:26 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-2016-8743	216.165.113.171	443	7/27/2017, 12:00:00 AM	3/10/2020, 4:01:08 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-2016-8743	128.238.182.14	80	7/27/2017, 12:00:00 AM	3/10/2020, 3:56:33 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	216.165.2.23	80	7/13/2017, 12:00:00 AM	3/10/2020, 3:52:31 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-2017-3737	34.196.167.182	80	12/7/2017, 12:00:00 AM	3/10/2020, 3:43:28 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3738	34.196.167.182	80	12/7/2017, 12:00:00 AM	3/10/2020, 3:43:28 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	34.196.167.182	80	11/2/2017, 12:00:00 AM	3/10/2020, 3:43:28 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-0703	128.122.128.23	443	3/2/2016, 12:00:00 AM	3/10/2020, 3:39:35 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2016-8743	128.122.128.23	443	7/27/2017, 12:00:00 AM	3/10/2020, 3:39:35 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-2016-8743	128.122.128.31	443	7/27/2017, 12:00:00 AM	3/10/2020, 3:32:50 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-2016-0703	128.122.128.31	443	3/2/2016, 12:00:00 AM	3/10/2020, 3:32:50 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-2016-8743	128.122.128.34	443	7/27/2017, 12:00:00 AM	3/10/2020, 3:32:38 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-2016-0703	128.122.128.34	443	3/2/2016, 12:00:00 AM	3/10/2020, 3:32:38 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-2017-7529	18.163.38.96	80	7/13/2017, 12:00:00 AM	3/10/2020, 3:26:56 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-2017-7529	128.122.85.97	443	7/13/2017, 12:00:00 AM	3/10/2020, 3:23:44 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-2014-3556	128.122.85.97	443	12/29/2014, 12:00:00 AM	3/10/2020, 3:23:44 AM
Vulnerability Description : The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.				
CVE-2016-4450	128.122.85.97	443	6/7/2016, 12:00:00 AM	3/10/2020, 3:23:44 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2015-3185	128.238.26.26	80	7/20/2015, 12:00:00 AM	3/10/2020, 3:21:40 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.238.26.26	80	7/20/2015, 12:00:00 AM	3/10/2020, 3:21:40 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.238.26.26	80	11/2/2017, 12:00:00 AM	3/10/2020, 3:21:40 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-0226	128.238.26.26	80	7/20/2014, 12:00:00 AM	3/10/2020, 3:21:40 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.238.26.26	80	12/7/2017, 12:00:00 AM	3/10/2020, 3:21:40 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	128.238.26.26	80	7/27/2017, 12:00:00 AM	3/10/2020, 3:21:40 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-2017-3737	128.238.26.26	80	12/7/2017, 12:00:00 AM	3/10/2020, 3:21:40 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	52.1.126.186	80	7/27/2017, 12:00:00 AM	3/10/2020, 3:19:16 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	128.238.66.155	80	7/13/2017, 12:00:00 AM	3/10/2020, 3:15:27 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-2017-7529	128.238.66.238	80	7/13/2017, 12:00:00 AM	3/10/2020, 2:53:58 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2017-7529	128.238.66.235	80	7/13/2017, 12:00:00 AM	3/10/2020, 2:34:08 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-2016-0703	128.238.66.31	443	3/2/2016, 12:00:00 AM	3/10/2020, 2:29:05 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-2016-8743	128.238.66.31	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:29:05 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-2016-8743	128.238.26.21	80	7/27/2017, 12:00:00 AM	3/10/2020, 2:27:52 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-2014-0226	128.238.26.21	80	7/20/2014, 12:00:00 AM	3/10/2020, 2:27:52 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.238.26.21	80	7/20/2015, 12:00:00 AM	3/10/2020, 2:27:52 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	128.238.26.21	80	7/20/2015, 12:00:00 AM	3/10/2020, 2:27:52 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.238.182.100	80	7/27/2017, 12:00:00 AM	3/10/2020, 2:15:56 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-2016-8743	149.56.24.26	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:15:14 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-2017-5647	91.230.41.24	443	4/17/2017, 12:00:00 AM	3/10/2020, 2:05:21 AM
Vulnerability Description : A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2017-12616	91.230.41.24	443	9/19/2017, 12:00:00 AM	3/10/2020, 2:05:21 AM
Vulnerability Description : When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.				
CVE-2017-5664	91.230.41.24	443	6/6/2017, 12:00:00 AM	3/10/2020, 2:05:21 AM
Vulnerability Description : The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.				
CVE-2017-12617	91.230.41.24	443	10/3/2017, 12:00:00 AM	3/10/2020, 2:05:21 AM
Vulnerability Description : When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.				
CVE-2016-8743	91.230.41.26	443	7/27/2017, 12:00:00 AM	3/10/2020, 2:03:35 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	34.192.88.207	80	7/13/2017, 12:00:00 AM	3/10/2020, 1:59:17 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-2016-4450	34.192.88.207	80	6/7/2016, 12:00:00 AM	3/10/2020, 1:59:17 AM
Vulnerability Description : os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.				
CVE-2016-0703	128.238.66.31	80	3/2/2016, 12:00:00 AM	3/10/2020, 1:37:40 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-2016-8743	128.238.66.31	80	7/27/2017, 12:00:00 AM	3/10/2020, 1:37:40 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-2016-8743	128.238.38.77	80	7/27/2017, 12:00:00 AM	3/10/2020, 1:32:08 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-2017-3736	52.1.187.2	80	11/2/2017, 12:00:00 AM	3/10/2020, 1:31:35 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	52.1.187.2	80	7/20/2015, 12:00:00 AM	3/10/2020, 1:31:35 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	52.1.187.2	80	7/27/2017, 12:00:00 AM	3/10/2020, 1:31:35 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-2015-3185	52.1.187.2	80	7/20/2015, 12:00:00 AM	3/10/2020, 1:31:35 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3738	52.1.187.2	80	12/7/2017, 12:00:00 AM	3/10/2020, 1:31:35 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	52.1.187.2	80	12/7/2017, 12:00:00 AM	3/10/2020, 1:31:35 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	52.1.187.2	80	7/20/2014, 12:00:00 AM	3/10/2020, 1:31:35 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	34.213.36.80	80	7/27/2017, 12:00:00 AM	3/10/2020, 1:25:26 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	216.165.2.15	80	7/13/2017, 12:00:00 AM	3/10/2020, 1:15:46 AM

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-3736	34.231.72.14	80	11/2/2017, 12:00:00 AM	3/10/2020, 12:42:12 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3737	34.231.72.14	80	12/7/2017, 12:00:00 AM	3/10/2020, 12:42:12 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3738	34.231.72.14	80	12/7/2017, 12:00:00 AM	3/10/2020, 12:42:12 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2016-8743	34.211.6.55	80	7/27/2017, 12:00:00 AM	3/10/2020, 12:12:59 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-2015-3185	128.122.51.6	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:11:45 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.51.6	443	7/20/2014, 12:00:00 AM	3/10/2020, 12:11:45 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.51.6	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:11:45 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.51.6	443	7/27/2017, 12:00:00 AM	3/10/2020, 12:11:45 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-3736	128.122.49.39	443	11/2/2017, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	128.122.49.39	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.39	443	7/20/2014, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.122.49.39	443	12/7/2017, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3183	128.122.49.39	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.49.39	443	7/27/2017, 12:00:00 AM	3/10/2020, 12:06:24 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-2017-3737	128.122.49.39	443	12/7/2017, 12:00:00 AM	3/10/2020, 12:06:24 AM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3737	128.122.122.243	443	12/7/2017, 12:00:00 AM	3/10/2020, 12:03:36 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.122.122.243	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:03:36 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.122.243	443	11/2/2017, 12:00:00 AM	3/10/2020, 12:03:36 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	128.122.122.243	443	12/7/2017, 12:00:00 AM	3/10/2020, 12:03:36 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.122.243	443	7/20/2014, 12:00:00 AM	3/10/2020, 12:03:36 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.122.243	443	7/20/2015, 12:00:00 AM	3/10/2020, 12:03:36 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.122.243	443	7/27/2017, 12:00:00 AM	3/10/2020, 12:03:36 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-2016-8743	91.230.41.214	80	7/27/2017, 12:00:00 AM	3/10/2020, 12:02:20 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-2015-3183	91.230.41.214	80	7/20/2015, 12:00:00 AM	3/10/2020, 12:02:20 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2015-3185	91.230.41.214	80	7/20/2015, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-3670	91.230.41.214	80	10/29/2014, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2015-0232	91.230.41.214	80	1/27/2015, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-3597	91.230.41.214	80	8/22/2014, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2014-0226	91.230.41.214	80	7/20/2014, 12:00:00 AM	3/10/2020, 12:02:20 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.238.63.10	80	12/7/2017, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.238.63.10	80	7/20/2014, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2014-3670	128.238.63.10	80	10/29/2014, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3737	128.238.63.10	80	12/7/2017, 12:00:00 AM	3/10/2020, 12:00:29 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.238.63.10	80	7/27/2017, 12:00:00 AM	3/10/2020, 12:00:29 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-2017-3736	128.238.63.10	80	11/2/2017, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-0232	128.238.63.10	80	1/27/2015, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2014-3597	128.238.63.10	80	8/22/2014, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-3185	128.238.63.10	80	7/20/2015, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.238.63.10	80	7/20/2015, 12:00:00 AM	3/10/2020, 12:00:29 AM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.238.63.26	80	7/27/2017, 12:00:00 AM	3/9/2020, 11:46:53 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-2016-8743	34.211.6.55	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:39:06 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-2016-8743	216.165.36.69	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:38:33 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2017-3737	128.122.109.53	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 11.0 is not affected.				
CVE-2017-3738	128.122.109.53	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 11.0-11.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 11.0 at this time. The fix will be included in OpenSSL 11.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	128.122.109.53	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.109.53	443	7/20/2014, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	128.122.109.53	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:36:54 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-2017-3736	128.122.109.53	443	11/2/2017, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 11.0 before 11.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.109.53	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:36:54 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.109.49	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:36:51 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2015-3183	128.238.182.23	80	7/20/2015, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-3670	128.238.182.23	80	10/29/2014, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.				
CVE-2017-3737	128.238.182.23	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.238.182.23	80	7/27/2017, 12:00:00 AM	3/9/2020, 11:35:47 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-2017-3738	128.238.182.23	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3736	128.238.182.23	80	11/2/2017, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2014-3597	128.238.182.23	80	8/22/2014, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2014-0226	128.238.182.23	80	7/20/2014, 12:00:00 AM	3/9/2020, 11:35:47 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-0232	128.238.182.23	80	1/27/2015, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2015-3185	128.238.182.23	80	7/20/2015, 12:00:00 AM	3/9/2020, 11:35:47 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2016-8743	128.122.109.62	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:29:46 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-2017-3738	128.122.49.29	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:26:41 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.29	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:26:41 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3185	128.122.49.29	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:26:41 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.29	443	7/20/2014, 12:00:00 AM	3/9/2020, 11:26:41 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2015-3183	128.122.49.29	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:26:41 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3736	128.122.49.29	443	11/2/2017, 12:00:00 AM	3/9/2020, 11:26:41 PM
Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.				

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.49.29	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:26:41 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-2016-8743	128.238.64.116	80	7/27/2017, 12:00:00 AM	3/9/2020, 11:25:40 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-2017-3736	18.182.119.242	80	11/2/2017, 12:00:00 AM	3/9/2020, 11:23:48 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	18.182.119.242	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:23:48 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	18.182.119.242	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:23:48 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-3597	128.122.49.27	443	8/22/2014, 12:00:00 AM	3/9/2020, 11:21:50 PM
Vulnerability Description : Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.				
CVE-2015-0232	128.122.49.27	443	1/27/2015, 12:00:00 AM	3/9/2020, 11:21:50 PM
Vulnerability Description : The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.				
CVE-2017-3737	128.122.49.27	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:21:50 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
<p>Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (<code>SSL_do_handshake()</code>, <code>SSL_accept()</code> and <code>SSL_connect()</code>), however due to a bug it does not work correctly if <code>SSL_read()</code> or <code>SSL_write()</code> is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If <code>SSL_read()</code>/<code>SSL_write()</code> is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to <code>SSL_read()</code>/<code>SSL_write()</code> being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</p>				
CVE-2017-3736	128.122.49.27	443	11/2/2017, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</p>				
CVE-2014-3670	128.122.49.27	443	10/29/2014, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : The <code>exif_ifd_make_value</code> function in <code>exif.c</code> in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the <code>exif_thumbnail</code> function.</p>				
CVE-2015-3183	128.122.49.27	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in <code>modules/http/http_filters.c</code>.</p>				
CVE-2015-3185	128.122.49.27	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : The <code>ap_some_auth_required</code> function in <code>server/request.c</code> in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a <code>Require</code> directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.</p>				
CVE-2016-8743	128.122.49.27	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>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 <code>httpd</code> participates in any chain of proxies or interacts with back-end application servers, either through <code>mod_proxy</code> or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.</p>				
CVE-2014-0226	128.122.49.27	443	7/20/2014, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : Race condition in the <code>mod_status</code> module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the <code>status_handler</code> function in <code>modules/generators/mod_status.c</code> and the <code>lua_ap_scoreboard_worker</code> function in <code>modules/lua/lua_request.c</code>.</p>				
CVE-2017-3738	128.122.49.27	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:21:50 PM
<p>Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.</p>				
CVE-2016-8743	128.238.63.13	80	7/27/2017, 12:00:00 AM	3/9/2020, 11:18:52 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
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-2016-8743	128.238.63.20	80	7/27/2017, 12:00:00 AM	3/9/2020, 11:16:09 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-2017-7529	34.198.67.142	443	7/13/2017, 12:00:00 AM	3/9/2020, 11:06:55 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-2016-8743	128.122.49.18	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:05:03 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-2017-3738	128.122.49.33	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:34 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2014-0226	128.122.49.33	443	7/20/2014, 12:00:00 AM	3/9/2020, 11:01:34 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3736	128.122.49.33	443	11/2/2017, 12:00:00 AM	3/9/2020, 11:01:34 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.49.33	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:01:34 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.49.33	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:01:34 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-2015-3185	128.122.49.33	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:01:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3737	128.122.49.33	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:34 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3737	128.122.49.30	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:25 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	128.122.49.30	443	7/27/2017, 12:00:00 AM	3/9/2020, 11:01:25 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-2015-3183	128.122.49.30	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:01:25 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.49.30	443	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:25 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	128.122.49.30	443	7/20/2015, 12:00:00 AM	3/9/2020, 11:01:25 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.30	443	7/20/2014, 12:00:00 AM	3/9/2020, 11:01:25 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3736	128.122.49.30	443	11/2/2017, 12:00:00 AM	3/9/2020, 11:01:25 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2017-3738	3.225.114.16	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:15 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	3.225.114.16	80	12/7/2017, 12:00:00 AM	3/9/2020, 11:01:15 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2017-3736	3.225.114.16	80	11/2/2017, 12:00:00 AM	3/9/2020, 11:01:15 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.238.64.107	80	7/27/2017, 12:00:00 AM	3/9/2020, 10:57:16 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-2016-8743	128.122.49.56	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:56:26 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-2017-3737	128.122.49.56	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:56:26 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2014-0226	128.122.49.56	443	7/20/2014, 12:00:00 AM	3/9/2020, 10:56:26 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3738	128.122.49.56	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:56:26 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2015-3185	128.122.49.56	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:56:26 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2017-3736	128.122.49.56	443	11/2/2017, 12:00:00 AM	3/9/2020, 10:56:26 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3183	128.122.49.56	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:56:26 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2017-3738	128.122.49.37	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.37	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2015-3183	128.122.49.37	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2015-3185	128.122.49.37	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2014-0226	128.122.49.37	443	7/20/2014, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3736	128.122.49.37	443	11/2/2017, 12:00:00 AM	3/9/2020, 10:55:21 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2016-8743	128.122.49.37	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:55:21 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-2014-0226	128.122.49.35	443	7/20/2014, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2017-3736	128.122.49.35	443	11/2/2017, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.				
CVE-2015-3185	128.122.49.35	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	128.122.49.35	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2016-8743	128.122.49.35	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:52:28 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
CVE-2017-3738	128.122.49.35	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.				
CVE-2017-3737	128.122.49.35	443	12/7/2017, 12:00:00 AM	3/9/2020, 10:52:28 PM
Vulnerability Description : OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.				
CVE-2016-8743	34.214.227.165	80	7/27/2017, 12:00:00 AM	3/9/2020, 10:46:16 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-2016-8743	128.122.65.146	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:45:43 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-2016-0703	128.122.65.146	443	3/2/2016, 12:00:00 AM	3/9/2020, 10:45:43 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-2016-8743	35.167.243.251	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:44:35 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-2016-8743	216.165.47.16	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:29:02 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-2015-3185	216.165.47.16	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:29:02 PM
Vulnerability Description : The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.				
CVE-2015-3183	216.165.47.16	443	7/20/2015, 12:00:00 AM	3/9/2020, 10:29:02 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

VULNERABILITY	IP ADDRESS	PORT	CVE PUBLISH DATE	LAST OBSERVED
Vulnerability Description : The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.				
CVE-2014-0226	216.165.47.16	443	7/20/2014, 12:00:00 AM	3/9/2020, 10:29:02 PM
Vulnerability Description : Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.				
CVE-2016-8743	216.165.47.90	443	7/27/2017, 12:00:00 AM	3/9/2020, 10:27:37 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.				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.



## 72 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	MEDIUM SEVERITY	LOW SEVERITY	POSITIVE
There are no High Severity Issues for Endpoint Security	Outdated Web Browser Observed 1,074	There are no Low Severity Issues for Endpoint Security	There are no Positive Signals for Endpoint Security
	Outdated Operating System Observed 1		
			There are no Informational Signals for Endpoint Security
INFORMATIONAL			

### !! Outdated Web Browser Observed

-2.1 SCORE IMPACT

An outdated web browser connected to a web server.

#### 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.

#### 500 findings

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	63.0.3239.84	end of service	78.0.3904.108	202.66.60.164	63691, 10109, 49500, 56115, 61022, 61023, 50333, 64122, 52805, 57579	3/12/2020, 4:00:00 AM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	192.76.177.125	49806, 49895, 57294, 6113, 36726, 24033	3/12/2020, 1:00:00 AM
Apple	Safari	9.1.2	end of service	13.0	216.165.126.19	2203, 3711, 51278	3/11/2020, 10:50:56 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.179	60259, 62192, 62986, 50906, 39008, 56948, 56731, 57597, 54033, 59092	3/11/2020, 10:45:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.113	32191, 43457	3/11/2020, 10:43:37 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.182	54289, 54564	3/11/2020, 10:23:38 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.148		3/11/2020, 10:18:45 PM
Apple	Safari	11.1	end of service	13.0	128.122.77.36		3/11/2020, 9:19:43 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.102	47077, 10752, 14385, 19156, 21336, 1750, 37872, 45972, 21364, 4489	3/11/2020, 9:15:03 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.128	58157	3/11/2020, 9:02:41 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.191.46	56818, 51762, 58508, 60772, 54994, 55661, 54019, 62956, 60217, 60275	3/11/2020, 9:00:28 PM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	128.122.92.12	53191, 59164, 61784, 61154, 65038, 51655, 53434, 53723	3/11/2020, 9:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.84	49636	3/11/2020, 9:00:00 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.138		3/11/2020, 8:52:44 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.126.118	34301, 15622, 34527, 23139, 44115, 28639, 29409, 48650, 4345, 10944	3/11/2020, 8:44:39 PM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	128.122.134.46	63353, 61732, 58310, 53032, 63819, 56558, 51583, 63695	3/11/2020, 8:00:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.191.62	59980, 53095, 53697, 54329, 51209, 51582, 55016, 53698, 49305, 55781	3/11/2020, 8:00:00 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.93.180		3/11/2020, 7:52:56 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.127.20		3/11/2020, 7:43:55 PM
Google	Chrome	58.6.3029.81	end of service	78.0.3904.108	91.230.41.204		3/11/2020, 7:35:59 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.85	4337	3/11/2020, 7:28:10 PM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	216.165.95.188		3/11/2020, 7:25:16 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.134		3/11/2020, 7:04:53 PM
Google	Chrome	55.0.2883.87	end of service	78.0.3904.108	216.165.95.166		3/11/2020, 7:04:29 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.95.58	63384, 63386, 63043, 53541, 53542, 51137, 64446, 65443, 60254, 54412	3/11/2020, 7:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	128.122.27.27	51454, 54913, 58164	3/11/2020, 7:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.179		3/11/2020, 6:55:22 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.143	52258, 54968, 25301, 49807, 49935, 60893, 14893, 56543, 49191, 62445	3/11/2020, 6:41:08 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.170		3/11/2020, 6:27:04 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.162		3/11/2020, 6:07:16 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.127.38	1819, 42453, 17676, 48606, 9169, 48401, 1311, 13263, 14119, 25531	3/11/2020, 6:04:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	55.0.2883.91	end of service	78.0.3904.108	216.165.126.19	33615	3/11/2020, 6:00:00 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.60.177	1185, 4366, 4630	3/11/2020, 5:48:57 PM
Google	Chrome	64.0.3282.119	end of service	78.0.3904.108	216.165.126.117	3716	3/11/2020, 5:44:11 PM
Apple	Safari	10.1.1	end of service	13.0	202.66.60.165	51955, 54731, 63244, 32470, 54071, 64865, 51465, 51530, 57064, 24301	3/11/2020, 5:00:00 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.126.122	1397	3/11/2020, 4:33:09 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.164		3/11/2020, 4:13:01 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.125	37808, 34119, 42642, 46062, 20469, 45261, 2390, 33667, 12063, 21917	3/11/2020, 4:00:00 PM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	216.165.95.190	49537, 50970, 51862, 55800	3/11/2020, 4:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.137	64813	3/11/2020, 3:08:41 PM
Mozilla	Firefox	45.0	end of service	70.0.1	216.165.126.25	29027, 8010, 19054, 39194, 37925, 39690, 47458, 30182, 52141, 29471	3/11/2020, 3:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.126.122	7264	3/11/2020, 2:28:21 PM
Google	Chrome	64.0.3282.140	end of service	78.0.3904.108	193.146.139.109		3/11/2020, 2:26:51 PM
Apple	Safari	11.1	end of service	13.0	192.114.110.38		3/11/2020, 2:17:55 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.178	62589, 50296, 30236	3/11/2020, 1:51:34 PM
Mozilla	Firefox	36.0	end of service	70.0.1	91.230.41.204		3/11/2020, 11:01:48 AM
Mozilla	Firefox	51.0	end of service	70.0.1	128.122.222.79		3/11/2020, 9:13:13 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	63.0.3239.84	end of service	78.0.3904.108	202.66.60.165	56534, 56953, 44871, 50938, 52335, 52295, 57105, 57110, 55971, 57109	3/11/2020, 9:00:00 AM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	202.66.60.165	53927, 34528, 49944, 51829, 30970, 53553, 62257, 50137, 50753, 5906	3/11/2020, 8:07:39 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.188	59830, 65284, 52710, 55182, 55202, 50237, 49761	3/11/2020, 7:27:48 AM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.172	63434	3/11/2020, 7:23:26 AM
Google	Chrome	49.0.2623.111	end of service	78.0.3904.108	216.165.125.249		3/11/2020, 5:36:13 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.131		3/11/2020, 3:54:14 AM
Google	Chrome	64.0.3282.186	end of service	78.0.3904.108	128.122.234.182		3/11/2020, 3:32:17 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.155	55840, 51063	3/11/2020, 3:01:34 AM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	128.122.122.142		3/11/2020, 2:12:16 AM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.151		3/11/2020, 12:09:55 AM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.143		3/11/2020, 12:06:55 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.166	50537, 50095, 51815, 51029, 27569, 60309, 61643, 51252, 32898, 51558	3/11/2020, 12:00:00 AM
Google	Chrome	60.0.3112.78	end of service	78.0.3904.108	216.165.95.161		3/10/2020, 11:58:40 PM
Apple	Safari	11.0.3	end of service	13.0	128.122.77.35		3/10/2020, 11:12:04 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Mozilla	Firefox	48.0	end of service	70.0.1	128.122.78.48	50253, 50728, 50934, 50410, 53906, 54938, 51129, 50469	3/10/2020, 11:00:00 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.154	49941, 54681, 49530, 50288	3/10/2020, 10:00:00 PM
Google	Chrome	61.0.3163.100	end of service	78.0.3904.108	216.165.95.189		3/10/2020, 9:55:55 PM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	216.165.95.147		3/10/2020, 9:33:54 PM
Google	Chrome	66.0.3359.170	end of service	78.0.3904.108	216.165.95.159		3/10/2020, 9:25:58 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.150		3/10/2020, 9:14:28 PM
Apple	Safari	10.1.2	end of service	13.0	192.114.110.38		3/10/2020, 9:00:50 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.131	61157, 62931, 64210, 64813, 17347, 63575, 63760, 65381, 49584, 49427	3/10/2020, 9:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.148	58806, 60681, 36991, 51060, 52734, 56957, 42134	3/10/2020, 9:00:00 PM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	216.165.95.170	55847	3/10/2020, 9:00:00 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.185		3/10/2020, 8:59:32 PM
Google	Chrome	66.0.3359.170	end of service	78.0.3904.108	216.165.95.174		3/10/2020, 8:58:12 PM
Google	Chrome	59.0.3071.112	end of service	78.0.3904.108	216.165.95.167		3/10/2020, 8:42:21 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.174	57805, 65154	3/10/2020, 8:35:25 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.183		3/10/2020, 8:09:04 PM
Apple	Safari	10.1.2	end of service	13.0	192.76.177.124		3/10/2020, 8:07:01 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.125.249		3/10/2020, 7:26:30 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.21.1	62761	3/10/2020, 7:24:20 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.130	62037, 62027, 60224	3/10/2020, 7:00:00 PM
Apple	Safari	6.1.6	end of service	13.0	216.165.95.173	51157, 51235	3/10/2020, 7:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.146	16186, 56748	3/10/2020, 7:00:00 PM
Apple	Safari	9.1.2	end of service	13.0	192.76.177.125		3/10/2020, 6:55:32 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.149	53705, 54524, 54214, 55779, 58679, 58404, 58966, 54763, 54966, 54241	3/10/2020, 6:46:47 PM
Mozilla	Firefox	52.0	end of service	70.01	128.122.92.159		3/10/2020, 6:26:40 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.167	24499	3/10/2020, 6:23:30 PM
Apple	Safari	10.0	end of service	13.0	216.165.95.184		3/10/2020, 6:11:56 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.167	49663, 57857, 61825, 14891, 7167, 64740, 64181, 59119, 53877, 56018	3/10/2020, 6:03:15 PM
Mozilla	Firefox	52.0	end of service	70.01	216.165.126.19	27113, 12244, 34808, 33998, 38346, 42758, 36489, 43329, 3408, 18564	3/10/2020, 6:00:00 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.176		3/10/2020, 5:35:43 PM
Mozilla	Firefox	52.0	end of service	70.01	216.165.95.191		3/10/2020, 4:52:40 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.105	12482	3/10/2020, 4:44:35 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.1	end of service	13.0	216.165.126.25	51789, 37535, 32415, 44461, 27068, 34302, 9789, 31037, 7276, 44416	3/10/2020, 4:40:42 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.172		3/10/2020, 4:38:45 PM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	216.165.95.173	49558	3/10/2020, 4:03:32 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.188	9629, 45775	3/10/2020, 3:57:12 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.126.103	3215, 2262, 43384, 43647, 26508, 30065, 52197, 31494, 27809, 32556	3/10/2020, 3:47:10 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.153		3/10/2020, 3:26:09 PM
Apple	Safari	9.1.1	end of service	13.0	216.165.95.161		3/10/2020, 3:17:44 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.146	17068, 52562	3/10/2020, 3:16:57 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.18		3/10/2020, 2:38:28 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.140	62311, 51732, 57503, 57693	3/10/2020, 2:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.25	22828, 22668, 42510, 2580, 8926, 1634, 50892, 43372, 28595, 32185	3/10/2020, 1:40:42 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.185	21472	3/10/2020, 1:12:52 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.183	55810, 50261	3/10/2020, 1:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.19	20000, 51984, 28069, 37900, 42612, 50453, 17214, 14184, 53191, 49223	3/10/2020, 12:53:28 PM
Apple	Safari	11.0.3	end of service	13.0	212.219.93.253		3/10/2020, 11:02:49 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.0.3	end of service	13.0	91.230.41.202	43104, 33013, 6444, 45886, 38432, 4642, 57949, 28826, 48457	3/10/2020, 10:49:35 AM
Opera Software	Opera	12.14	end of service	65.0.3467.42	202.66.60.164		3/10/2020, 9:24:57 AM
Microsoft	Internet Explorer	8.0	end of service	11.0.145	128.122.55.10		3/10/2020, 8:27:13 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.191		3/10/2020, 7:13:58 AM
Google	Chrome	63.0.3239.84	end of service	78.0.3904.108	128.122.182.140		3/10/2020, 5:16:15 AM
Google	Chrome	54.0.2840.99	end of service	78.0.3904.108	216.165.95.164		3/10/2020, 5:13:32 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.140	33354	3/10/2020, 5:00:00 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.162	52901, 59207, 50116, 57654, 57111, 61650, 59498, 59000, 58485, 62115	3/10/2020, 4:00:00 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.177		3/10/2020, 3:12:02 AM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	216.165.95.164		3/10/2020, 2:54:35 AM
Google	Chrome	55.0.2883.87	end of service	78.0.3904.108	216.165.95.164		3/10/2020, 2:49:51 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.135	65485, 65294, 51217	3/10/2020, 2:41:46 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.177	64671, 64808, 64638, 52373, 65074, 58419, 59460, 54933, 51788, 55415	3/10/2020, 2:26:47 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.182	51653, 52050, 54138, 53536	3/10/2020, 2:00:00 AM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.128	64701, 64477, 55084, 55087, 56923, 51817, 14322, 55929, 53231, 62931	3/10/2020, 2:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.1	end of service	13.0	216.165.126.19	21090, 22916, 33029, 50857, 22666, 16796, 21391, 17771, 19244, 39136	3/10/2020, 2:00:00 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.177		3/10/2020, 1:08:10 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.181	62753, 14965, 54071, 54980, 51988, 54601, 50400, 51177, 61968, 64645	3/10/2020, 1:00:00 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.152	51698, 50203, 56136	3/10/2020, 1:00:00 AM
Apple	Safari	10.0.3	end of service	13.0	216.165.95.188		3/10/2020, 12:48:53 AM
Apple	Safari	10.0.3	end of service	13.0	216.165.95.130		3/10/2020, 12:47:48 AM
Apple	Safari	10.1	end of service	13.0	216.165.95.165		3/10/2020, 12:46:56 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.145		3/10/2020, 12:31:10 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.154	65487	3/10/2020, 12:27:59 AM
Google	Chrome	61.0.3163.100	end of service	78.0.3904.108	216.165.95.139		3/10/2020, 12:18:51 AM
Apple	Safari	11.1	end of service	13.0	128.122.77.34		3/10/2020, 12:00:03 AM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	216.165.95.155	58986	3/10/2020, 12:00:00 AM
Apple	Safari	10.1.2	end of service	13.0	192.76.177.125		3/9/2020, 11:56:45 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.142	58356, 63411, 54388	3/9/2020, 11:44:24 PM
Google	Chrome	60.0.3112.78	end of service	78.0.3904.108	216.165.95.131		3/9/2020, 11:39:14 PM
Google	Chrome	60.0.3112.101	end of service	78.0.3904.108	216.165.95.142	59082	3/9/2020, 11:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.154	30225	3/9/2020, 11:00:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.184		3/9/2020, 10:18:27 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.149	51147	3/9/2020, 10:00:00 PM
Apple	Safari	6.1.6	end of service	13.0	216.165.95.175	51822	3/9/2020, 10:00:00 PM
Apple	Safari	6.1.6	end of service	13.0	216.165.95.142	51929	3/9/2020, 10:00:00 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.153		3/9/2020, 9:53:12 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.126.25		3/9/2020, 9:46:40 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.169	13666, 63198, 63873, 62522, 61717, 10750, 54367, 57220, 17946, 53493	3/9/2020, 9:25:56 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.133	55978, 63851, 62273, 53285	3/9/2020, 9:09:48 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.140	61453, 49554, 49432, 50477, 55755, 58820, 56624, 54823, 58555, 58816	3/9/2020, 9:00:01 PM
Apple	Safari	9.1	end of service	13.0	216.165.95.132		3/9/2020, 8:35:29 PM
Mozilla	Firefox	59.0	end of service	70.01	216.165.95.146		3/9/2020, 8:35:21 PM
Google	Chrome	63.0.3239.108	end of service	78.0.3904.108	216.165.95.161		3/9/2020, 8:33:27 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.176	59945	3/9/2020, 8:15:44 PM
Apple	Safari	10.0	end of service	13.0	216.165.95.168		3/9/2020, 8:00:22 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.176	23742, 54422, 57608, 9151, 58936, 58879, 50569, 61810, 57684, 27099	3/9/2020, 7:52:04 PM
Google	Chrome	51.0.2704.106	end of service	78.0.3904.108	216.165.95.176		3/9/2020, 7:43:03 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Mozilla	Firefox	57.0	end of service	70.0.1	128.122.77.39	55156, 18636, 8099, 29791, 46912	3/9/2020, 7:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.130		3/9/2020, 6:49:24 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.160	62275	3/9/2020, 6:34:28 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.127.12		3/9/2020, 6:23:48 PM
Google	Chrome	55.0.2883.95	end of service	78.0.3904.108	216.165.95.138		3/9/2020, 6:06:33 PM
Google	Chrome	54.0.2840.99	end of service	78.0.3904.108	216.165.95.138		3/9/2020, 6:04:43 PM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	216.165.95.153	49902, 45155	3/9/2020, 6:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	128.122.160.65	51416, 51577, 50564, 53604, 55385, 57176, 56921, 59628, 62974, 62716	3/9/2020, 6:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	128.122.167.74	59646	3/9/2020, 6:00:00 PM
Microsoft	Internet Explorer	6.0	end of service	11.0.145	128.122.55.177		3/9/2020, 5:37:13 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.190		3/9/2020, 5:17:48 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.129	60561	3/9/2020, 5:14:59 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.184		3/9/2020, 5:13:49 PM
Google	Chrome	60.0.3112.113	end of service	78.0.3904.108	216.165.126.122	5448	3/9/2020, 5:00:00 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.129	11647	3/9/2020, 5:00:00 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.182	12284, 55527, 57410, 57968, 57454	3/9/2020, 4:45:02 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.191		3/9/2020, 4:25:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.0.2	end of service	13.0	216.165.95.137		3/9/2020, 4:07:02 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.135	51622, 51949, 63473, 59391, 64281	3/9/2020, 4:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.127.12		3/9/2020, 3:28:41 PM
Mozilla	Firefox	36.0	end of service	70.0.1	128.122.174.74		3/9/2020, 3:22:14 PM
Google	Chrome	60.0.3112.113	end of service	78.0.3904.108	216.165.95.170		3/9/2020, 3:21:34 PM
Google	Chrome	59.0.3071.115	end of service	78.0.3904.108	91.230.41.202	39798, 24465, 36375, 22289, 49515, 22572, 33072, 41776, 56582, 16885	3/9/2020, 3:11:51 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.146		3/9/2020, 2:54:24 PM
Apple	Safari	11.1	end of service	13.0	212.219.93.253		3/9/2020, 1:20:47 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.126.18	1307, 3618, 42142, 13042, 3362, 3142, 12849, 8711, 52914, 38041	3/9/2020, 1:20:44 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.92.121		3/9/2020, 1:17:59 PM
Apple	Safari	10.1.2	end of service	13.0	91.230.41.204	19984, 13230	3/9/2020, 11:37:47 AM
Google	Chrome	60.0.3112.90	end of service	78.0.3904.108	91.230.41.202	45986, 50374, 25191	3/9/2020, 8:42:20 AM
Microsoft	Internet Explorer	7.0	end of service	11.0.145	128.122.170.239		3/9/2020, 8:34:13 AM
Apple	Safari	11.0.2	end of service	13.0	91.230.41.204	37115	3/9/2020, 8:00:00 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.130		3/9/2020, 7:20:33 AM
Google	Chrome	62.0.3202.62	end of service	78.0.3904.108	216.165.95.136	64376	3/9/2020, 7:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.1	end of service	13.0	216.165.95.191	8876	3/9/2020, 6:43:29 AM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.167	49841	3/9/2020, 6:00:00 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.138	51652	3/9/2020, 2:24:28 AM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.171		3/9/2020, 2:22:19 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.187	50865, 52775, 52491	3/9/2020, 2:00:01 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.162	61441	3/9/2020, 2:00:00 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.141		3/9/2020, 1:43:37 AM
Mozilla	Firefox	45.0	end of service	70.0.1	128.122.238.224		3/9/2020, 1:30:14 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.157	62506, 61274	3/9/2020, 12:40:00 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.144		3/8/2020, 11:24:03 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.131	55270	3/8/2020, 10:00:00 PM
Apple	Safari	10.0.3	end of service	13.0	216.165.95.173		3/8/2020, 9:44:31 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.189	61427	3/8/2020, 8:22:47 PM
Apple	Safari	11.0	end of service	13.0	216.165.95.151	51262, 55349	3/8/2020, 8:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.138		3/8/2020, 7:54:23 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.173		3/8/2020, 7:52:08 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.158	63083, 62010, 52876	3/8/2020, 6:18:30 PM
Mozilla	Firefox	53.0	end of service	70.0.1	91.230.41.204		3/8/2020, 6:09:43 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.0.1	end of service	13.0	91.230.41.202	46684, 9368, 8315	3/8/2020, 1:46:01 PM
Opera Software	Opera	12.14	end of service	65.0.3467.42	202.66.60.165	56327	3/8/2020, 11:33:30 AM
Apple	Safari	9.1.2	end of service	13.0	91.230.41.202		3/8/2020, 11:00:18 AM
Mozilla	Firefox	46.0	end of service	70.0.1	91.230.41.204		3/8/2020, 10:43:03 AM
Apple	Safari	9.0.3	end of service	13.0	91.230.41.204		3/8/2020, 7:30:50 AM
Apple	Safari	11.0.2	end of service	13.0	128.122.119.236		3/8/2020, 6:40:17 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.132	53533, 53748, 54577, 53050, 62653, 63059, 59324, 7512, 51740, 50022	3/8/2020, 6:00:00 AM
Google	Chrome	55.0.2883.95	end of service	78.0.3904.108	216.165.95.151		3/8/2020, 5:54:55 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.148	64977, 50318, 59008, 27532	3/8/2020, 4:52:07 AM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	202.66.60.164	56729, 35054, 51249	3/8/2020, 4:10:27 AM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.126.93	5611, 7820, 17918, 7913, 44138, 43587, 23545, 36955, 27925, 44244	3/8/2020, 4:00:00 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.174	65235	3/8/2020, 2:54:00 AM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	128.122.248.183		3/8/2020, 2:53:14 AM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	128.122.92.64		3/8/2020, 1:32:17 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.142		3/8/2020, 12:34:57 AM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	216.165.126.103	7904, 36777	3/8/2020, 12:07:10 AM
Apple	Safari	10.1	end of service	13.0	216.165.95.151		3/8/2020, 12:00:22 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	60.0.3112.90	end of service	78.0.3904.108	128.122.139.87		3/7/2020, 11:33:16 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.149		3/7/2020, 11:32:43 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.158		3/7/2020, 10:07:07 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.171	52878, 50607, 62264, 57214	3/7/2020, 10:00:00 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.187	65268	3/7/2020, 10:00:00 PM
Google	Chrome	41.0.2225.0	end of service	78.0.3904.108	216.165.95.86		3/7/2020, 9:35:04 PM
Google	Chrome	54.0.2840.98	end of service	78.0.3904.108	216.165.95.174		3/7/2020, 9:22:20 PM
Mozilla	Firefox	3.0.1	end of service	70.0.1	128.122.214.120		3/7/2020, 9:01:51 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.153	52421, 9765, 64602	3/7/2020, 9:00:00 PM
Apple	Safari	10.0	end of service	13.0	216.165.95.188	57160	3/7/2020, 8:14:09 PM
Google	Chrome	39.0.2171.95	end of service	78.0.3904.108	216.165.95.170		3/7/2020, 8:06:34 PM
Apple	Safari	11.1	end of service	13.0	192.76.177.125	63740, 51865	3/7/2020, 8:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.147	63620, 50565	3/7/2020, 7:36:59 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.176	64597, 33763, 58716	3/7/2020, 7:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.170	50373, 51579, 60766, 59043	3/7/2020, 6:44:11 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.179	62897, 64719, 52127, 52826, 46684	3/7/2020, 5:57:01 PM
Apple	Safari	11.1	end of service	13.0	80.250.25.114		3/7/2020, 4:15:19 PM
Apple	Safari	10.0.3	end of service	13.0	202.66.60.164	64599	3/7/2020, 4:00:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	63.0.3239.84	end of service	78.0.3904.108	216.165.95.165		3/7/2020, 3:57:14 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.156		3/7/2020, 3:22:44 PM
Apple	Safari	10.1.1	end of service	13.0	192.114.110.38		3/7/2020, 2:29:41 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.176	56460, 54640, 50701, 49758, 50458, 10610, 63317, 18080, 65327, 46731	3/7/2020, 7:13:21 AM
Apple	Safari	10.1.1	end of service	13.0	202.66.60.164	3080, 35733, 60532, 50677, 60378, 60672, 60101, 60969, 60873, 60273	3/7/2020, 7:12:12 AM
Mozilla	Firefox	56.0	end of service	70.01	128.122.77.32	13625	3/7/2020, 7:00:00 AM
Apple	Safari	11.0.1	end of service	13.0	192.76.177.124	49938	3/7/2020, 6:54:16 AM
Apple	Safari	10.0.1	end of service	13.0	216.165.95.133		3/7/2020, 6:22:27 AM
Apple	Safari	11.0.1	end of service	13.0	202.66.60.165		3/7/2020, 6:20:10 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.185	26603, 58286, 58418	3/7/2020, 6:00:00 AM
Apple	Safari	10.0.2	end of service	13.0	128.122.77.39	61536	3/7/2020, 5:00:28 AM
Apple	Safari	10.0	end of service	13.0	216.165.95.148		3/7/2020, 1:50:58 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.150	58259, 52871, 59530, 64903	3/6/2020, 11:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.167	50743, 14714, 52732	3/6/2020, 10:54:36 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.154	54393	3/6/2020, 10:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.169		3/6/2020, 9:56:29 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.165		3/6/2020, 9:29:42 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	128.122.7.43		3/6/2020, 9:25:53 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.134	31412, 53739, 10542, 53252, 51049, 52475, 52072	3/6/2020, 9:00:00 PM
Google	Chrome	58.0.3029.81	end of service	78.0.3904.108	216.165.95.169	37576	3/6/2020, 9:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	91.230.41.202	33168, 51520, 26526, 43254, 17421, 35845, 56000, 45944, 2053, 35293	3/6/2020, 8:46:24 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.154	51185, 50427, 56128, 50419, 50073, 57108, 61170, 55916, 62749, 49847	3/6/2020, 8:40:28 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	128.122.51.242		3/6/2020, 8:11:18 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.95.133	36427	3/6/2020, 8:00:00 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.165		3/6/2020, 7:36:36 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.95.184		3/6/2020, 7:12:28 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.161	54208, 49558, 61403	3/6/2020, 6:57:15 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.138	51671	3/6/2020, 6:56:08 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.126.19		3/6/2020, 6:53:53 PM
Apple	Safari	10.0	end of service	13.0	216.165.95.143	59400, 59703, 59946, 56401, 60143	3/6/2020, 6:37:06 PM
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	128.122.59.192	55503	3/6/2020, 6:32:59 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.135		3/6/2020, 6:23:46 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.149		3/6/2020, 6:10:51 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	9.1.3	end of service	13.0	216.165.95.130		3/6/2020, 5:50:23 PM
Mozilla	Firefox	48.0	end of service	70.0.1	216.165.95.166		3/6/2020, 5:05:15 PM
Apple	Safari	9.0.3	end of service	13.0	216.165.95.173	40894, 55804	3/6/2020, 5:00:00 PM
Microsoft	Internet Explorer	5.5	end of service	11.0.145	128.122.58.154		3/6/2020, 4:33:16 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.173	56448, 39847	3/6/2020, 4:00:00 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.160		3/6/2020, 3:56:31 PM
Apple	Safari	11.1	end of service	13.0	216.165.126.117	45472, 38851, 35306, 21866	3/6/2020, 3:52:25 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.133		3/6/2020, 3:41:46 PM
Apple	Safari	11.1	end of service	13.0	91.230.41.202	59269, 6352	3/6/2020, 3:30:10 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.126.102	42443, 20553, 35632, 14764, 29462, 34571, 49066, 52529	3/6/2020, 3:00:00 PM
Apple	Safari	6.1.6	end of service	13.0	216.165.95.135	50970, 51069	3/6/2020, 3:00:00 PM
Apple	Safari	6.1.6	end of service	13.0	216.165.95.160	56244, 50665	3/6/2020, 3:00:00 PM
Google	Chrome	60.0.3112.90	end of service	78.0.3904.108	216.165.95.136		3/6/2020, 2:46:56 PM
Apple	Safari	9.1.3	end of service	13.0	91.230.41.202		3/6/2020, 2:34:17 PM
Apple	Safari	9.1.2	end of service	13.0	91.230.41.204	40593, 41342, 29476	3/6/2020, 2:02:27 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.181		3/6/2020, 1:59:30 PM
Google	Chrome	60.0.3112.113	end of service	78.0.3904.108	91.230.41.204		3/6/2020, 1:37:20 PM
Google	Chrome	47.0.2626.106	end of service	78.0.3904.108	202.66.60.165		3/6/2020, 12:12:15 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	63.0.3239.108	end of service	78.0.3904.108	91.230.41.202		3/6/2020, 10:08:53 AM
Microsoft	Edge	12.246	end of service	44.18362.449.0	128.122.100.70		3/6/2020, 4:37:13 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.183		3/6/2020, 4:34:31 AM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	202.66.60.165		3/6/2020, 4:24:38 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.175	64900, 62417, 51078	3/6/2020, 3:46:35 AM
Google	Chrome	62.0.3202.94	end of service	78.0.3904.108	202.66.60.165		3/6/2020, 2:44:32 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.128	62172	3/6/2020, 2:41:21 AM
Google	Chrome	63.0.3219.0	end of service	78.0.3904.108	216.165.95.152		3/6/2020, 2:39:16 AM
Apple	Safari	11.1	end of service	13.0	216.165.126.18	9080, 34432, 35682, 22017, 4584, 27353, 22323, 4376, 47430, 26114	3/6/2020, 2:32:19 AM
Apple	Safari	11.1	end of service	13.0	128.122.77.38	39218	3/6/2020, 2:00:00 AM
Google	Chrome	63.0.3235.0	end of service	78.0.3904.108	216.165.95.160	61125	3/6/2020, 1:00:00 AM
Google	Chrome	60.0.3112.113	end of service	78.0.3904.108	216.165.95.147		3/6/2020, 12:28:00 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.168	64767	3/6/2020, 12:19:05 AM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.151		3/6/2020, 12:04:03 AM
Opera Software	Opera	12.14	end of service	65.0.3467.42	216.165.95.134		3/5/2020, 11:55:08 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.160	63843, 53180	3/5/2020, 11:53:17 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.187	64511	3/5/2020, 11:13:20 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.186	62074	3/5/2020, 11:07:10 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.135	55491	3/5/2020, 11:00:00 PM
Mozilla	Firefox	57.0	end of service	70.0.1	216.165.126.19	19439, 4610, 10823, 7996, 16377, 30869, 49174, 32856, 10386, 41337	3/5/2020, 11:00:00 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.173		3/5/2020, 10:58:06 PM
Google	Chrome	60.0.3112.101	end of service	78.0.3904.108	216.165.95.159		3/5/2020, 10:31:36 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.140		3/5/2020, 10:27:25 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.132	65195	3/5/2020, 10:05:52 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.126.19	13399, 48798, 36579, 44084, 1423, 36571, 33150, 53234, 24267, 42228	3/5/2020, 10:00:00 PM
Google	Chrome	63.0.3239.84	end of service	78.0.3904.108	216.165.95.179		3/5/2020, 9:47:36 PM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	216.165.95.158		3/5/2020, 9:25:03 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.186		3/5/2020, 9:20:41 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.176	23895, 54700	3/5/2020, 9:00:00 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.92.180		3/5/2020, 8:58:26 PM
Apple	Safari	11.0	end of service	13.0	216.165.95.167		3/5/2020, 8:55:11 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.163	55732, 54926, 61968, 54632	3/5/2020, 8:34:28 PM
Mozilla	Firefox	47.0	end of service	70.0.1	216.165.95.166		3/5/2020, 7:48:06 PM
Google	Chrome	63.0.3239.108	end of service	78.0.3904.108	216.165.95.137		3/5/2020, 7:46:32 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.173		3/5/2020, 7:43:52 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.144	49343	3/5/2020, 7:41:40 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.129		3/5/2020, 7:37:01 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.126.103		3/5/2020, 7:09:36 PM
Mozilla	Firefox	48.0	end of service	70.0.1	128.122.230.148		3/5/2020, 6:50:03 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.161		3/5/2020, 5:58:51 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.127.20		3/5/2020, 5:52:11 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.165		3/5/2020, 5:21:56 PM
Apple	Safari	11.0	end of service	13.0	216.165.126.125	11140, 40892, 27366, 52701, 33212, 42263, 27148, 32424, 29183, 52953	3/5/2020, 5:19:11 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.135		3/5/2020, 4:28:17 PM
Apple	Safari	6.0.2	end of service	13.0	216.165.126.25	41485	3/5/2020, 4:25:42 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.190		3/5/2020, 4:13:04 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.185	25092	3/5/2020, 4:07:45 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.129	50307, 17842, 54050	3/5/2020, 4:05:58 PM
Google	Chrome	64.0.3282.186	end of service	78.0.3904.108	216.165.95.188	49489	3/5/2020, 4:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.151	55810, 42920, 50174	3/5/2020, 4:00:00 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.189		3/5/2020, 3:39:06 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	63.0.3239.132	end of service	78.0.3904.108	128.122.204.194		3/5/2020, 3:38:49 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.145	50237, 49732, 64994, 52577, 61720, 53199, 50135, 64836, 65341, 49619	3/5/2020, 3:13:19 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.144	58537	3/5/2020, 3:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.178	59477, 65452, 33807, 58945, 56352	3/5/2020, 3:00:00 PM
Apple	Safari	10.0.1	end of service	13.0	216.165.95.156		3/5/2020, 2:57:52 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.171	50819	3/5/2020, 2:49:08 PM
Google	Chrome	57.0.2987.98	end of service	78.0.3904.108	202.66.60.165		3/5/2020, 2:42:40 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.95.139		3/5/2020, 2:40:54 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	128.122.230.140		3/5/2020, 1:40:16 PM
Apple	Safari	11.0.1	end of service	13.0	91.230.41.202		3/5/2020, 1:32:41 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.177		3/5/2020, 11:42:35 AM
Apple	Safari	10.1.2	end of service	13.0	202.66.60.164		3/5/2020, 8:31:35 AM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	202.66.60.164		3/5/2020, 7:35:55 AM
Mozilla	Firefox	52.0	end of service	70.0.1	91.230.41.204		3/5/2020, 7:25:08 AM
Apple	Safari	11.0.1	end of service	13.0	91.230.41.204	21626, 59083	3/5/2020, 6:52:45 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.144	62896, 57092	3/5/2020, 5:08:30 AM
Apple	Safari	11.0	end of service	13.0	216.165.95.163	50478	3/5/2020, 5:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.0.1	end of service	13.0	216.165.95.171		3/5/2020, 4:49:13 AM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	216.165.95.190		3/5/2020, 3:18:09 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.131	65392, 58158	3/5/2020, 2:47:14 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.175		3/5/2020, 2:41:21 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.170	24359, 57392, 53953, 53094	3/5/2020, 2:33:33 AM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.150		3/5/2020, 2:32:19 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.189	53439, 53243, 60997, 54364, 58740, 39795, 55167, 59403, 45873, 17886	3/5/2020, 2:30:08 AM
Apple	Safari	10.1	end of service	13.0	216.165.95.169		3/5/2020, 1:49:18 AM
Google	Chrome	62.0.3202.94	end of service	78.0.3904.108	202.66.60.164		3/5/2020, 1:36:22 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.165	63013, 21702	3/5/2020, 1:24:58 AM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.174		3/5/2020, 12:52:26 AM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.187		3/4/2020, 10:39:30 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.152	50901, 60867	3/4/2020, 10:37:31 PM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	216.165.95.185	65318	3/4/2020, 10:00:00 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.163		3/4/2020, 9:41:11 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.128		3/4/2020, 9:08:43 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.144	65078, 47371	3/4/2020, 8:56:25 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	9.1.2	end of service	13.0	216.165.95.169		3/4/2020, 8:27:09 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.166		3/4/2020, 8:26:09 PM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.167		3/4/2020, 8:01:06 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.140		3/4/2020, 7:02:29 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.126.18		3/4/2020, 6:53:32 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.179	51216, 60804, 53809, 56050, 65497, 27099, 53375, 56870, 24761, 57851	3/4/2020, 6:00:00 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.95.161	50389	3/4/2020, 6:00:00 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.185		3/4/2020, 5:57:14 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.173	49400, 61113, 61037, 53145, 27958, 23066, 51297, 19190, 64837, 62369	3/4/2020, 5:32:24 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	216.165.95.130		3/4/2020, 5:01:55 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.139	49498, 57847, 57234, 58156	3/4/2020, 4:33:53 PM
Mozilla	Firefox	52.0	end of service	70.01	216.165.95.163	58649, 54959, 54961	3/4/2020, 4:29:09 PM
Google	Chrome	54.0.2840.99	end of service	78.0.3904.108	216.165.95.178		3/4/2020, 4:28:28 PM
Mozilla	Firefox	52.0	end of service	70.01	216.165.95.161		3/4/2020, 4:27:20 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.131	10215, 59894, 59895, 63951	3/4/2020, 4:14:40 PM
Apple	Safari	9.1.3	end of service	13.0	216.165.126.102	41554, 43409	3/4/2020, 4:00:00 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.157	64661, 58743, 62595, 63777, 52590, 62959, 51441, 59036, 57801, 60282	3/4/2020, 3:59:36 PM
Microsoft	Internet Explorer	6.0	end of service	11.0.145	128.122.160.188		3/4/2020, 3:51:59 PM
Opera Software	Opera	12.14	end of service	65.0.3467.42	202.66.60.168		3/4/2020, 2:59:14 PM
Mozilla	Firefox	34.0	end of service	70.0.1	128.122.60.139		3/4/2020, 1:30:21 PM
Apple	Safari	10.0	end of service	13.0	212.219.93.253		3/4/2020, 1:27:45 PM
Apple	Safari	10.1.2	end of service	13.0	202.66.60.165		3/4/2020, 1:06:00 PM
Apple	Safari	11.0.2	end of service	13.0	91.230.41.202		3/4/2020, 11:27:14 AM
Mozilla	Firefox	42.0	end of service	70.0.1	128.122.121.66		3/4/2020, 9:32:13 AM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.172		3/4/2020, 8:37:21 AM
Mozilla	Firefox	41.0	end of service	70.0.1	128.122.250.216		3/4/2020, 5:29:13 AM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.133	61311	3/4/2020, 4:57:49 AM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.166		3/4/2020, 4:54:29 AM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.154		3/4/2020, 4:47:38 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.143		3/4/2020, 4:02:11 AM
Apple	Safari	11.0	end of service	13.0	216.165.95.171		3/4/2020, 3:46:36 AM
Microsoft	Internet Explorer	8.0	end of service	11.0.145	216.165.95.168		3/4/2020, 3:01:51 AM
Apple	Safari	11.0	end of service	13.0	216.165.95.159		3/4/2020, 1:44:40 AM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.1	end of service	13.0	216.165.95.136	63814, 26019, 54935, 57565, 59482, 60444, 59997, 50444	3/4/2020, 1:00:00 AM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.188		3/4/2020, 12:55:35 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.184	58117, 49773, 59279, 59322, 59881, 58861, 52384, 54360, 60562, 60404	3/4/2020, 12:47:40 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.126.122		3/3/2020, 11:54:11 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.170		3/3/2020, 11:53:52 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.153		3/3/2020, 11:45:46 PM
Microsoft	Edge	13.10586	end of service	44.18362.449.0	128.122.209.23		3/3/2020, 11:11:17 PM
Google	Chrome	60.0.3112.78	end of service	78.0.3904.108	216.165.95.138		3/3/2020, 11:07:31 PM
Google	Chrome	62.0.3202.94	end of service	78.0.3904.108	128.122.162.50	55969, 59060, 63610, 61314, 62556, 61271	3/3/2020, 11:00:00 PM
Microsoft	Edge	14.14393	end of service	44.18362.449.0	216.165.95.129	31387	3/3/2020, 11:00:00 PM
Google	Chrome	60.0.3112.90	end of service	78.0.3904.108	216.165.126.18	42860	3/3/2020, 11:00:00 PM
Apple	Safari	11.0	end of service	13.0	216.165.95.190		3/3/2020, 10:58:46 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.137		3/3/2020, 10:15:01 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.169	58839	3/3/2020, 10:00:00 PM
Mozilla	Firefox	52.0	end of service	70.01	128.122.93.94	55659, 59636	3/3/2020, 10:00:00 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.133	58615, 61818, 56545	3/3/2020, 10:00:00 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.130	13117, 56043	3/3/2020, 9:54:50 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.141	60688, 59224, 60981	3/3/2020, 9:00:00 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.143		3/3/2020, 8:53:44 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.94.31		3/3/2020, 8:45:31 PM
Mozilla	Firefox	56.0	end of service	70.0.1	216.165.95.163		3/3/2020, 8:40:22 PM
Google	Chrome	60.0.3112.113	end of service	78.0.3904.108	91.230.41.202		3/3/2020, 8:34:23 PM
Mozilla	Firefox	52.0	end of service	70.0.1	128.122.95.83	51395, 57303	3/3/2020, 8:03:55 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.134	63501, 62885, 16629, 62839, 53902, 50283, 52784, 52407, 52273, 60619	3/3/2020, 8:00:37 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.136	62342, 61486	3/3/2020, 8:00:00 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.146		3/3/2020, 7:58:14 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.128	49297	3/3/2020, 7:15:19 PM
Apple	Safari	11.1	end of service	13.0	192.76.177.124	51128	3/3/2020, 7:00:00 PM
Google	Chrome	54.0.2840.99	end of service	78.0.3904.108	216.165.95.171		3/3/2020, 6:33:06 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.157		3/3/2020, 6:32:13 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.164		3/3/2020, 6:26:03 PM
Google	Chrome	61.0.3163.100	end of service	78.0.3904.108	216.165.95.163		3/3/2020, 6:22:40 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.183		3/3/2020, 6:18:25 PM
Mozilla	Firefox	47.0	end of service	70.0.1	216.165.95.139		3/3/2020, 6:16:08 PM

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	10.1.2	end of service	13.0	216.165.95.136	56924	3/3/2020, 6:08:36 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.132		3/3/2020, 6:04:47 PM
Google	Chrome	51.0.2704.103	end of service	78.0.3904.108	216.165.126.106	20656, 6939, 21395, 25491, 13481, 31500, 26893, 40003, 6736, 34324	3/3/2020, 6:02:28 PM
Google	Chrome	49.0.2623.112	end of service	78.0.3904.108	91.230.41.204		3/3/2020, 5:53:05 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.151		3/3/2020, 5:50:21 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.162		3/3/2020, 5:26:54 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.126.19	38409, 14197, 10741, 41418, 31214, 12624, 6739, 20894, 8128, 44969	3/3/2020, 5:15:02 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.171	51210, 51717	3/3/2020, 5:00:04 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.158	64239, 49692, 49749, 49693, 50195, 50230, 49850, 50019, 49885, 50162	3/3/2020, 4:57:57 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.161		3/3/2020, 4:31:41 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.126.125		3/3/2020, 4:24:34 PM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.166		3/3/2020, 4:22:33 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.184		3/3/2020, 4:16:11 PM
Apple	Safari	9.1.2	end of service	13.0	216.165.95.139		3/3/2020, 4:05:16 PM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	216.165.95.175		3/3/2020, 3:35:05 PM
Google	Chrome	65.0.3325.181	end of service	78.0.3904.108	216.165.95.187	65354, 58789, 57792, 25456	3/3/2020, 3:31:43 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Google	Chrome	59.0.3071.115	end of service	78.0.3904.108	91.230.41.204	47846, 62960, 10405	3/3/2020, 3:11:09 PM
Apple	Safari	10.0.1	end of service	13.0	216.165.95.179	49400	3/3/2020, 3:00:00 PM
Mozilla	Firefox	52.0	end of service	70.0.1	216.165.95.157		3/3/2020, 2:48:46 PM
Google	Chrome	56.0.2924.87	end of service	78.0.3904.108	216.165.95.163		3/3/2020, 2:04:47 PM
Apple	Safari	10.1.2	end of service	13.0	128.122.77.39	56320, 36523	3/3/2020, 2:00:00 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.126.85		3/3/2020, 1:53:28 PM
Google	Chrome	59.0.3071.115	end of service	78.0.3904.108	128.122.205.76		3/3/2020, 1:06:14 PM
Google	Chrome	59.0.3071.104	end of service	78.0.3904.108	216.165.95.86	55734, 63846	3/3/2020, 1:00:00 PM
Apple	Safari	10.0.3	end of service	13.0	216.165.126.102		3/3/2020, 11:48:22 AM
Google	Chrome	57.0.2987.110	end of service	78.0.3904.108	91.230.41.202		3/3/2020, 9:50:44 AM
Microsoft	Internet Explorer	7.0	end of service	11.0.145	128.122.25.247		3/3/2020, 8:33:14 AM
Apple	Safari	10.1.1	end of service	13.0	91.230.41.202		3/3/2020, 8:02:07 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.153	54538	3/3/2020, 7:00:00 AM
Apple	Safari	11.1	end of service	13.0	91.230.41.204	11906, 50107	3/3/2020, 6:56:33 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.146	43432, 58457, 61014	3/3/2020, 6:52:28 AM
Mozilla	Firefox	15.0.1	end of service	70.0.1	128.122.215.75		3/3/2020, 6:43:18 AM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.132	65238	3/3/2020, 5:00:00 AM
Google	Chrome	66.0.3359.181	end of service	78.0.3904.108	216.165.95.180	45933	3/3/2020, 4:00:00 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Apple	Safari	11.0.1	end of service	13.0	216.165.95.150		3/3/2020, 3:40:49 AM
Mozilla	Firefox	56.0	end of service	70.0.1	216.165.95.145		3/3/2020, 1:31:41 AM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.186	59194, 42644, 54579	3/3/2020, 1:28:14 AM
Google	Chrome	60.0.3112.78	end of service	78.0.3904.108	216.165.95.182		3/3/2020, 1:04:07 AM
Apple	Safari	11.1	end of service	13.0	216.165.95.155	63852, 58528, 60290	3/3/2020, 1:00:00 AM
Apple	Safari	11.0.3	end of service	13.0	216.165.95.178		3/3/2020, 12:39:26 AM
Apple	Safari	10.0.2	end of service	13.0	216.165.95.146		3/3/2020, 12:20:18 AM
Apple	Safari	11.0	end of service	13.0	216.165.95.182		3/3/2020, 12:00:45 AM
Mozilla	Firefox	45.0	end of service	70.0.1	216.165.126.18	25634, 10291, 46618, 4454, 35992, 43934	3/2/2020, 10:59:40 PM
Apple	Safari	11.0.1	end of service	13.0	216.165.95.164		3/2/2020, 10:59:22 PM
Apple	Safari	10.1	end of service	13.0	216.165.95.153		3/2/2020, 10:50:50 PM
Apple	Safari	10.1.1	end of service	13.0	216.165.95.181	57469	3/2/2020, 10:25:09 PM
Apple	Safari	10.1.2	end of service	13.0	216.165.95.172	60300	3/2/2020, 10:15:05 PM
Google	Chrome	62.0.3202.75	end of service	78.0.3904.108	216.165.95.136	65289, 61241	3/2/2020, 10:00:00 PM
Google	Chrome	62.0.3202.94	end of service	78.0.3904.108	192.76.177.125	59456, 18015	3/2/2020, 10:00:00 PM
Apple	Safari	11.0.2	end of service	13.0	216.165.95.187		3/2/2020, 9:58:48 PM
Apple	Safari	10.0.2	end of service	13.0	192.76.177.125		3/2/2020, 9:11:13 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.166	52053, 51871, 8432, 63721	3/2/2020, 8:51:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MANUFACTURER	PRODUCT	VERSION	STATUS	LATEST VERSION	SOURCE IP	PORTS	LAST OBSERVED
Mozilla	Firefox	37.0	end of service	70.0.1	128.122.183.75		3/2/2020, 8:40:13 PM
Mozilla	Firefox	48.0	end of service	70.0.1	216.165.95.141	59727	3/2/2020, 8:00:00 PM
Apple	Safari	11.1	end of service	13.0	216.165.95.168	50749, 59382	3/2/2020, 8:00:00 PM

## !! Outdated Operating System Observed

-1.0 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

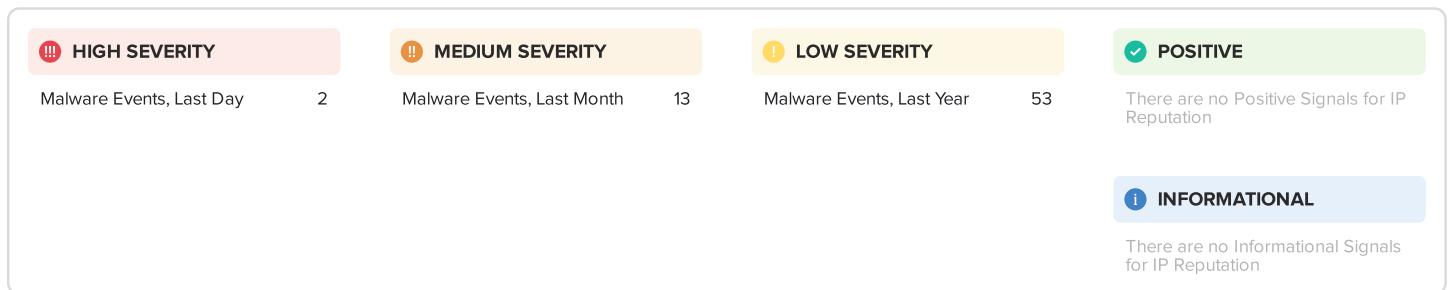
Update affected device's operating system. Enable automatic updates if available from your software vendor and permitted in your environment. Maintain a regular update schedule for all software and hardware in use within your organization, ensuring that all the latest patches are applied soon after they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

1 finding

MANUFACTURER	PRODUCT	VERSION	STATUS	SOURCE IP	PORTS	LAST OBSERVED
Microsoft	Windows 98		end of service	128.122.58.154		3/6/2020, 4:33:16 PM

 **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 the Malware Exposure Key Threat Indicator.



## Malware Events, Last Year

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.

### Recommendation

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

53 findings

MALWARE FAMILY	TYPE	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
qrypter.rat	bot	sinkhole	216.165.2.133	4	3/9/2020, 10:58:41 AM
generic	bot	sinkhole	202.66.60.164	1	3/8/2020, 10:47:32 AM
nivdort	bot	sinkhole	216.165.95.84	1	3/7/2020, 10:05:04 PM
adware.android.imp	bot	sinkhole	203.174.165.232	1	3/5/2020, 3:03:39 AM
adware.android.imp	bot	sinkhole	80.250.25.114	1	3/1/2020, 3:10:26 PM
minr	bot	sinkhole	216.165.95.181	1	2/28/2020, 11:44:16 PM
adware.android.imp	bot	sinkhole	216.165.95.163	1	2/27/2020, 9:56:26 PM
adware.android.imp	bot	sinkhole	212.219.93.253	1	2/26/2020, 3:34:25 PM

MALWARE FAMILY	TYPE	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
stealrat	bot	email	216.165.95.86	2	2/25/2020, 8:38:18 PM
adware.am15	bot	sinkhole	216.165.95.153	1	2/18/2020, 8:01:34 PM
unknown3014	bot	email	216.165.95.84	1	2/14/2020, 12:06:46 AM
adware.android.imp	bot	sinkhole	91.230.41.204	1	2/10/2020, 8:25:47 AM
nymaim	bot	sinkhole	216.165.95.143	220	2/10/2020, 2:55:43 AM
adware.am15	bot	sinkhole	216.165.95.162	1	2/8/2020, 2:33:58 AM
generic	bot	sinkhole	128.238.182.22	348	1/29/2020, 6:55:39 PM
nymaim	bot	sinkhole	192.76.177.124	346	1/25/2020, 4:51:34 PM
android.dianshangsale	bot	sinkhole	91.230.41.204	19	1/25/2020, 9:39:25 AM
adware.am15	bot	sinkhole	202.66.60.168	2	1/21/2020, 1:50:18 AM
nymaim	bot	sinkhole	202.66.60.165	265	1/14/2020, 9:53:22 AM
android.dianshangsale	bot	sinkhole	216.165.125.249	68	1/13/2020, 11:07:51 PM
android.dianshangsale	bot	sinkhole	216.165.127.20	8	1/12/2020, 10:59:23 AM
nymaim	bot	sinkhole	202.66.60.164	341	1/7/2020, 11:37:25 AM
qqblack	bot	sinkhole	202.66.60.168	12	12/30/2019, 1:07:34 PM
adware.android.erosuper	bot	sinkhole	202.66.60.167	9	12/4/2019, 1:07:46 AM
wrokn1	bot	sinkhole	91.230.41.204	5	11/30/2019, 5:54:30 PM
qqblack	bot	sinkhole	202.66.60.169	20	11/23/2019, 4:33:24 PM
emotet	bot	email	193.146.139.109	360	11/4/2019, 10:23:48 AM
sshauth	bot	other	216.165.113.154	371	10/27/2019, 5:45:25 PM
andromeda	bot	sinkhole	216.165.125.249	446	10/22/2019, 7:52:10 PM
trojan.iframe	bot	sinkhole	202.66.60.168	1	10/1/2019, 5:59:37 PM
wrokn1	bot	sinkhole	91.230.41.202	2	9/26/2019, 6:47:44 PM
lethic	bot	sinkhole	128.122.77.35	1	9/24/2019, 3:36:17 AM
andromeda	bot	sinkhole	192.76.177.125	498	9/23/2019, 1:38:12 AM
trojan.iframe	bot	sinkhole	192.76.177.125	6	9/19/2019, 6:44:29 PM
cryptoloot	bot	sinkhole	202.66.60.166	3	9/19/2019, 3:44:56 AM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

MALWARE FAMILY	TYPE	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
cryptoloot	bot	sinkhole	216.165.95.189	1	9/4/2019, 10:07:10 PM
coinminer	bot	sinkhole	216.165.95.167	1	9/4/2019, 8:32:01 PM
coinminer	bot	sinkhole	216.165.95.150	1	9/3/2019, 6:02:31 PM
gamut	bot	email	202.66.60.169	1357	8/10/2019, 4:31:25 PM
cryptoloot	bot	sinkhole	202.66.60.168	1	8/9/2019, 7:32:44 AM
gamut	bot	email	202.66.60.168	1298	8/8/2019, 5:25:37 AM
gamut	bot	email	59.79.127.27	950	8/4/2019, 5:18:10 PM
cryptoloot	bot	sinkhole	202.66.60.169	1	7/31/2019, 10:06:09 AM
pua.sprotector	bot	sinkhole	216.165.95.190	2	7/19/2019, 4:38:49 PM
android.uupay	bot	sinkhole	202.66.60.167	23	5/31/2019, 2:59:13 AM
android.uupay	bot	sinkhole	202.66.60.166	5	5/12/2019, 5:05:59 AM
lethic	bot	sinkhole	193.175.54.224	1	4/30/2019, 7:44:09 AM
nymaim	bot	sinkhole	3.92.1.50	331	4/26/2019, 1:58:48 AM
nymaim	bot	sinkhole	128.122.215.13	350	4/11/2019, 11:01:50 PM
other	bot	sinkhole	128.122.50.148	347	3/6/2019, 7:53:27 PM
other	bot	sinkhole	216.165.95.132	347	3/6/2019, 5:52:37 PM
other	bot	sinkhole	128.122.50.158	349	3/5/2019, 8:15:04 PM
nymaim	bot	sinkhole	128.122.215.16	496	3/4/2019, 12:30:02 AM

## !! Malware Events, Last Month

-2.7 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.

13 findings

MALWARE FAMILY	TYPE	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
qrypter.rat	bot	sinkhole	216.165.2.133	4	3/9/2020, 10:58:41 AM
generic	bot	sinkhole	202.66.60.164	1	3/8/2020, 10:47:32 AM
nivdort	bot	sinkhole	216.165.95.84	1	3/7/2020, 10:05:04 PM
adware.android.imp	bot	sinkhole	203.174.165.232	1	3/5/2020, 3:03:39 AM
adware.android.imp	bot	sinkhole	80.250.25.114	1	3/1/2020, 3:10:26 PM
minr	bot	sinkhole	216.165.95.181	1	2/28/2020, 11:44:16 PM
adware.android.imp	bot	sinkhole	216.165.95.163	1	2/27/2020, 9:56:26 PM
adware.android.imp	bot	sinkhole	212.219.93.253	1	2/26/2020, 3:34:25 PM
stealrat	bot	email	216.165.95.86	2	2/25/2020, 8:38:18 PM
adware.am15	bot	sinkhole	216.165.95.153	1	2/18/2020, 8:01:34 PM
unknown3014	bot	email	216.165.95.84	1	2/14/2020, 12:06:46 AM
nymaim	bot	sinkhole	216.165.95.143	220	2/10/2020, 2:55:43 AM
generic	bot	sinkhole	128.238.182.22	348	1/29/2020, 6:55:39 PM

## !!! Malware Events, Last Day

Communications indicative of malware infections were observed over the last 24 hours.

### 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	TYPE	DETECTION METHOD	SOURCE IP	OBSERVATIONS	INFECTION LAST OBSERVED
generic	bot	sinkhole	202.66.60.164	1	3/8/2020, 10:47:32 AM
stealrat	bot	email	216.165.95.86	2	2/25/2020, 8:38:18 PM

## D 69 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	MEDIUM SEVERITY	LOW SEVERITY	POSITIVE
There are no High Severity Issues for DNS Health	SPF Record Missing 74	SPF Record Contains a Softfail 2	There are no Positive Signals for DNS Health
			<b>INFORMATIONAL</b> There are no Informational Signals for DNS Health
			<b>-0.5</b> SCORE IMPACT

### ! SPF Record Contains a Softfail

Softfail attributes in SPF makes spoofing and phishing email possible.

#### Description

The Sender Policy Framework (SPF) is an email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record allows a receiving email server to validate that the inbound email comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record in the form of a TXT record. An SPF record with soft fail has been detected; the soft fail attribute enables spoofed email from the domain.

#### Recommendation

To resolve this issue, enumerate the list of email servers that are authorized to send email on behalf of the domain. Update the SPF record with the correct email authorization list.

#### 2 findings

DOMAIN	SPF RECORD	LAST OBSERVED
nyu.edu	v=spf1 ip4:128.122.0.0/16 ip4:216.165.0.0/17 ip4:199.91.136.26/32 ip4:199.91.140.26/32 ip4:72.55.140.81/32 include:spf- 00256a01.phhosted.com include:_spf.google.com include:sendgrid.net ip4:205.201.128.0/20 ip4:198.2.128.0/18 ip4:148.105.8.0/21 include:hobsonsmail.com ip4:139.60.152.0/22 ip4:162.247.216.0/22 ip4:54.186.193.102/32 ip4:52.222.73.120/32 ip4:52.222.73.83/32 ip4:52.222.62.51/32 ip4:52.222.75.85/32 ip4:34.194.230.233/32 ip4:34.230.107.215/32 ~all	3/10/2020, 2:18:42 AM

DOMAIN	SPF RECORD	LAST OBSERVED
nyu.edu	v=spf1 ip4:128.122.0.0/16 ip4:216.165.0.0/17 ip4:199.91.136.26/32 ip4:199.91.140.26/32 ip4:72.55.140.81/32 "include:spf- 00256a01.phhosted.com include:_spf.google.com include:sendgrid.net ip4:205.201.128.0/20 ip4:198.2.128.0/18 ip4:148.105.8.0/21 "include:hobsonsmail.com ip4:139.60.152.0/22 ip4:162.247.216.0/22 ip4:54.186.193.102/32 ip4:52.222.73.120/32 ip4:52.222.73.83/32 ip4:52.222.62.51/32 ip4:52.222.75.85/32 ip4:34.194.230.233/32 ip4:34.230.107.215/32 ~all	2/29/2020, 4:30:14 PM

## !! SPF Record Missing

-1.7 SCORE IMPACT

A missing SPF record has been detected for a domain.

### Description

The Sender Policy Framework (SPF) is a simple but effective email-validation technique designed to detect the forgery of email (also called email spoofing). An SPF record is a mechanism that allows a receiving email server to validate that inbound email from a particular domain comes from a server that is authorized to send email on behalf of that particular domain. The list of authorized sending hosts for a domain is published as a Domain Name System (DNS) record for that domain in the form of a specially formatted TXT record. An SPF record is required for spoofed e-mail prevention and anti-spam control.

### Recommendation

Create a valid Sender Policy Framework (SPF) record. Ensure the configuration of the SPF DNS record to verify syntax and MTA servers. Test the configuration to make sure its valid by checking the header of an incoming email looking for "spf=pass" Allow for DNS caching during testing; it may take up to 48 hours to fully propagate across the Internet. The nature of the SMTP protocol does not allow for complete prevention of spoofed emails, however the SPF header will reveal whether the email is authentic.

## 74 findings

DOMAIN	LAST OBSERVED
nyubraces.com	3/10/2020, 2:24:19 AM
livewellnyu.info	3/10/2020, 2:24:19 AM
nyuwireless.org	3/10/2020, 2:24:19 AM
nyuscps.org	3/10/2020, 2:24:18 AM
nyujade.org	3/10/2020, 2:24:18 AM
livewellnyu.us	3/10/2020, 2:24:18 AM
wnyu.org	3/10/2020, 2:24:18 AM
nyu.net	3/10/2020, 2:24:18 AM
nyu.info	3/10/2020, 2:24:15 AM
nyumobile.com	3/10/2020, 2:24:15 AM

DOMAIN	LAST OBSERVED
nyucareers.com	3/10/2020, 2:24:14 AM
nyuad-artscenter.org	3/10/2020, 2:24:14 AM
nyuscps.com	3/10/2020, 2:24:14 AM
livewellnyu.mobi	3/10/2020, 2:24:14 AM
nyualumni.com	3/10/2020, 2:24:14 AM
nyu.org	3/10/2020, 2:24:14 AM
livewellnyu.net	3/10/2020, 2:24:14 AM
nyux.org	3/10/2020, 2:24:14 AM
nyuniversity.nyc	3/10/2020, 2:24:14 AM
livewellnyu.org	3/10/2020, 2:24:13 AM
gonyuad.com	3/10/2020, 2:24:13 AM
nyuonline.com	3/10/2020, 2:24:13 AM
livewellnyu.biz	3/10/2020, 2:24:13 AM
gonyuathletics.com	3/10/2020, 2:24:13 AM
livewellnyu.com	3/10/2020, 2:24:13 AM
nyuapps.com	3/10/2020, 2:24:13 AM
nyu.biz	3/10/2020, 2:24:13 AM
nyufilmscoring.info	2/29/2020, 8:38:31 PM
nyufilm.info	2/29/2020, 8:38:31 PM
nyustudentfilm.info	2/29/2020, 8:37:48 PM
filmnyu.info	2/29/2020, 8:37:47 PM
nyugradschool.info	2/29/2020, 8:37:47 PM
nyugpa.info	2/29/2020, 8:36:09 PM
nyuclinic.info	2/29/2020, 8:36:09 PM
hotelsnearnyu.info	2/29/2020, 8:36:05 PM
nyumaster.info	2/29/2020, 8:36:05 PM
nyudesign.info	2/29/2020, 8:34:29 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	LAST OBSERVED
classesnyuedu.info	2/29/2020, 8:34:28 PM
nyutransfer.info	2/29/2020, 8:34:28 PM
nyuenrollment.info	2/29/2020, 8:34:12 PM
nyubusinessschool.info	2/29/2020, 8:34:12 PM
nyucost.info	2/29/2020, 8:34:12 PM
nyugraduateschool.info	2/29/2020, 8:34:12 PM
nyubusiness.info	2/29/2020, 8:34:12 PM
nyufilmdepartment.info	2/29/2020, 8:34:11 PM
nyuprograms.info	2/29/2020, 8:34:11 PM
filmcenternyu.info	2/29/2020, 8:34:10 PM
nyutischfilm.info	2/29/2020, 4:42:24 PM
nyucollege.info	2/29/2020, 4:42:24 PM
nyufilmstudies.info	2/29/2020, 4:42:23 PM
nyuschools.info	2/29/2020, 4:40:50 PM
nyugradfilm.info	2/29/2020, 4:40:49 PM
nyutheatre.info	2/29/2020, 4:40:49 PM
nyucantorfilm.info	2/29/2020, 4:40:49 PM
nyuapplication.info	2/29/2020, 4:40:48 PM
nyumedicalschool.info	2/29/2020, 4:40:48 PM
nyusummerfilm.info	2/29/2020, 4:40:48 PM
nyuhighschool.info	2/29/2020, 4:40:48 PM
nyulawschool.info	2/29/2020, 4:40:48 PM
nyugraduateprograms.info	2/29/2020, 4:40:47 PM
nyudrama.info	2/29/2020, 4:40:46 PM
nyufreshman.info	2/29/2020, 4:38:47 PM
nyushortfilm.info	2/29/2020, 4:38:47 PM
nyunewyork.info	2/29/2020, 4:38:47 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	LAST OBSERVED
nyustatistics.info	2/29/2020, 4:38:47 PM
filmschoolnyu.info	2/29/2020, 4:38:44 PM
classesatnyu.info	2/29/2020, 4:36:17 PM
nyundergroundfilm.info	2/29/2020, 4:36:17 PM
uscnyu.info	2/29/2020, 4:36:16 PM
nyugraduatefilm.info	2/29/2020, 4:36:16 PM
nyufilmfestival.info	2/29/2020, 4:36:16 PM
nyuart.info	2/29/2020, 4:33:19 PM
nyufilmprogram.info	2/29/2020, 4:30:13 PM
nyusummerclasses.info	2/29/2020, 4:30:10 PM

## 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	!! MEDIUM SEVERITY	! LOW SEVERITY	✓ POSITIVE
There are no High Severity Issues for Social Engineering	There are no Medium Severity Issues for Social Engineering	There are no Low Severity Issues for Social Engineering	There are no Positive Signals for Social Engineering
<b>i INFORMATIONAL</b>			There are no Informational Signals for Social Engineering

No issues found



## 72 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	MEDIUM SEVERITY	LOW SEVERITY	POSITIVE
Site does not enforce HTTPS 7	Website does not implement X-Frame-Options Best Practices 21	Website does not implement X-Content-Type-Options Best Practices 26	Web Application Firewall (WAF) Detected 16
	Website does not implement X-XSS-Protection Best Practices 26		
	Redirect Chain Contains HTTP 4		
	Website Does Not Implement HSTS Best Practices 34		
	Insecure HTTPS Redirect Pattern 5		
INFORMATIONAL			
	Website Hosted on Object Storage 1		
	Content Security Policy Contains Broad Directives 2		
	Website References Object Storage 6		
	Content Security Policy (CSP) Missing 26		
	Content Security Policy Contains 'unsafe-*' Directive 2		
	Unsafe Implementation Of Subresource Integrity 17		

### Website does not implement X-Frame-Options Best Practices

-0.3 SCORE IMPACT

Not explicitly setting X-Frame-Options allows other, untrusted, websites to embed your site in a frame on their page. This can be used to make social engineering attacks appear more legitimate, or can even be used for clickjacking attacks.

#### Description

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a '<frame>', '<iframe>' or '<object>'. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other websites.

#### Recommendation

Add one of the following headers, using the 'DENY' or 'ALLOW-FROM' directive, to responses from this website: X-Frame-Options: DENY X-Frame-Options: ALLOW-FROM https://example.com/

#### 21 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	Header missing	3/2/2020, 8:14:58 PM

Evidence :

nyuwireless.org	http://ftp.nyuwireless.org/	http://ftp.nyuwireless.org/	n/a	Header missing	3/2/2020, 8:14:58 PM
-----------------	-----------------------------	-----------------------------	-----	----------------	----------------------

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
livewellnyu.org	https://www.livewellnyu.org/	https://collegehealthqi.nyu.edu/	https://www.livewellnyu.org/, 301, https://collegehealthqi.nyu.edu/	Header missing	3/2/2020, 8:14:57 PM
Evidence :					
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	Header missing	3/2/2020, 8:14:53 PM
Evidence :					
gonyuad.com	https://www.gonyuad.com/	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/index, 302, https://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:52 PM
Evidence :					
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:50 PM
Evidence :					
nyualumni.com	https://video.nyualumni.com/	http://video.alumni.nyu.edu	https://video.nyualumni.com/, 302, http://video.alumni.nyu.edu	Header missing	3/2/2020, 8:14:48 PM
Evidence :					
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	Header missing	3/2/2020, 8:14:47 PM
Evidence :					
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	Header missing	3/2/2020, 8:14:46 PM
Evidence :					
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	Header missing	3/2/2020, 8:14:44 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
gonyuad.com	http://gonyuad.com/landing/index	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
nyu.edu	http://archive.nyu.edu/	https://archive.nyu.edu/	http://archive.nyu.edu/, 302, https://archive.nyu.edu/	Header missing	3/2/2020, 8:10:38 PM
Evidence :					
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	Header missing	3/2/2020, 8:10:35 PM
Evidence :					
nyu.edu	http://login.nyu.edu/	https://login.nyu.edu/	http://login.nyu.edu/, 302, https://login.nyu.edu/	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://cs.nyu.edu/	https://cs.nyu.edu/	http://cs.nyu.edu/, 301, https://cs.nyu.edu/	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:32 PM

Evidence :

## ! Website does not implement X-Content-Type-Options Best Practices

-0.1 SCORE IMPACT

Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. For example, an attacker could hide malicious code with an image extension, where the browser does introspection and executes it as JavaScript.

### Description

A MIME type is an HTTP header that indicates the type of content returned in a response and how it should be handled and displayed by the browser. Browsers will sometimes analyze the content themselves and handle it counter to the MIME type header; this can lead to security issues and execution of malicious code. The X-Content-Type-Options header indicates that browsers should always trust the declared MIME type from the server and not attempt to analyze the content themselves.

### Recommendation

Add the following header to responses from this website: 'X-Content-Type-Options: nosniff'

## 26 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&ltmpl=default&ltmplcache=2&emr=1&osid=1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVLJTsMwEL0j8Q%2BW71kahISJqiAEJVYojblwM0448SVYweP3cLfk6atCge4Pr95y3im15%2BdJhtwqKzJ6SROKQEjbK1Mk9NVdR9d0evi%2FGyKvNM9mwXfmgV8BEBPhkmDbHzlaXCGWY4KmeEdlPOCLWdPjyyLU9Y7	Header missing	3/2/2020, 8:15:01 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
			662wmpL5XU6NFLqFv pG6U807rAVIYaVW%2 FVqJWigldS3XLW8pet 3Gynax5ogB5gY9N36 A0iyN0osozaosZZOUX Vy%2BUVlenG6U2Tf4L 9b7noTsoarKqHxZVqP ARtXgngd2ThtrGw2xs N3OvuSlajPAkmsESma l4PwQ8NYaDB24JbiNE rBaPOa09b5HliTb7TY %2BySQ8MV8hhjokXC AtxrWysZn7sc%2F%2Fc %2FOjLy1OytPkhlRx%2 BK5di%2FIdabUSX2S mtd3eOuB%2BqOBdG BrcW9dx%2F7fbJJ6Mi KojOVJZMNiDUFJBTUI S7F1%2F38VwLd8%3D &RelayState=https%3A %2F%2Fwww.google.c om%2Fa%2Fnyu.edu% 2FServiceLogin%3Fser vice%3Dmail%26passiv e%3Dtrue%26rm%3Dfa lse%26continue%3Dhtt ps%253A%252F%252F mail.google.com%252 Fmail%252F%26ss%3D 1%26ltmpl%3Ddefault% 26ltmplcache%3D2%2 6emr%3D1%26osid%3 D1, 302, <a href="https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1">https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1</a>		

Evidence :

nyuwireless.org	http://calendar.nyuwireless.org/	https://calendar.nyuwireless.org/	http://calendar.nyuwireless.org/, 302, <a href="https://calendar.nyuwireless.org/">https://calendar.nyuwireless.org/</a>	Header missing	3/2/2020, 8:15:00 PM
-----------------	----------------------------------	-----------------------------------	---	----------------	----------------------

Evidence :

nyuwireless.org	https://files.nyuwireless.org/	https://files.nyuwireless.org/	n/a	Header missing	3/2/2020, 8:14:58 PM
-----------------	--------------------------------	--------------------------------	-----	----------------	----------------------

Evidence :

nyuwireless.org	http://files.nyuwireless.org/	http://files.nyuwireless.org/	n/a	Header missing	3/2/2020, 8:14:58 PM
-----------------	-------------------------------	-------------------------------	-----	----------------	----------------------

Evidence :

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	Header missing	3/2/2020, 8:14:58 PM
Evidence :					
nyuwireless.org	http://ftp.nyuwireless.org/	http://ftp.nyuwireless.org/	n/a	Header missing	3/2/2020, 8:14:58 PM
Evidence :					
livewellnyu.org	https://www.livewellnyu.org/	https://collegehealthqi.nyu.edu/	https://www.livewellnyu.org/, 301, https://collegehealthqi.nyu.edu/	Header missing	3/2/2020, 8:14:57 PM
Evidence :					
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	Header missing	3/2/2020, 8:14:53 PM
Evidence :					
gonyuad.com	https://www.gonyuad.com/	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/index, 302, https://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:52 PM
Evidence :					
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:50 PM
Evidence :					
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	Header missing	3/2/2020, 8:14:47 PM
Evidence :					
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	Header missing	3/2/2020, 8:14:46 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	Header missing	3/2/2020, 8:14:44 PM
Evidence :					
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
nyu.edu	http://archive.nyu.edu/	https://archive.nyu.edu/	http://archive.nyu.edu/, 302, https://archive.nyu.edu/	Header missing	3/2/2020, 8:10:38 PM
Evidence :					
nyu.edu	http://m.nyu.edu/	https://m.nyu.edu/default/nyu_app_index/index	http://m.nyu.edu/, 301, https://m.nyu.edu/, 302, https://m.nyu.edu/default/nyu_app_index/index	Header missing	3/2/2020, 8:10:36 PM
Evidence :					
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	Header missing	3/2/2020, 8:10:35 PM
Evidence :					
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	http://login.nyu.edu/	https://login.nyu.edu/	http://login.nyu.edu/, 302, https://login.nyu.edu/	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://cs.nyu.edu/	https://cs.nyu.edu/	http://cs.nyu.edu/, 301, https://cs.nyu.edu/	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:32 PM
Evidence :					

## i Website Hosted on Object Storage

Many object storage services offer hosting for a website's static assets. Amazon S3's documentation can be found at <https://docs.aws.amazon.com/AmazonS3/latest/dev/WebsiteHosting.html>.

### Description

There is no risk in using object storage services in this fashion. However, if the Access Control List (ACL) on the bucket (storage partition) the website is hosted on is misconfigured, then the website may be compromised or defaced by attackers.

### Recommendation

Ensure that the usage of external services, such as Amazon S3, conforms to company policies.

### 1 finding

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	Server header in HTTP response indicates website is hosted on Amazon S3	3/2/2020, 8:10:33 PM
Evidence : Server: AmazonS3					

## i Content Security Policy Contains Broad Directives

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

**Description**

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from loading resources on your page from domains that you don't explicitly trust. However, by using overly broad methods of describing what you trust (ie. 'http:', '\*', 'http://\*') for your script-src and object-src directives, or your default-src directive in the absence of those directives, this key feature of the CSP header can be bypassed by an attacker.

**Recommendation**

Explicitly specify trusted sources for your script-src and object-src policies. Ideally you can use the 'self' directive to limit scripts and objects to only those on your own domain, or you can explicitly specify domains that you trust and rely upon for your site to function.

2 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
--------	-------------	-----------	---------------	---------------

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin? service=mail&passive=true& rm=false&continue=https://mail.google.com/mail/&ss=1&lt mpl=default&ltmplcache=2& emr=1&osid=1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SS O? SAMLRequest=fVLJTsMwEL 0j8Q%2BW71kahISsJqiAEJV YojblwM0448SVYweP3cLfk6 atCge4Pr95y3im15%2BdJht wqKzJ6SROKQEjbK1Mk9NV dR9d0evi%2FGyKvNM9mwX fmgV8BEBPhkmDbHzlaXCG WY4KmeEdlPOCLWdPjyyLU 9Y7662wmpL5XU6NFLqFvp G6U807rAVIYaVW%2FVqJW iglds3XLW8peT3Gynax5ogB 5gY9N36A0iyN0osozaosZZ OUXVv%2BUVlenG6U2Tf4L 9b7noTsoarKqHxZVqPARtXg ngd2ThtrGw2xsN3OvuSlajP AkmsESmal4PwQ8NYaDB2 4JbiNErBaPOa09b5HliTb7T Y%2BySQ8MV8hhjokXCAtxr WysZn7sc%2F%2Fc%2FOjLy1 OytPk1Rx%2BK5di%2Fdab USX2Smtd3eOuB%2BqOBd GBrcW9dx%2F7fbJJ6MiKoj OVJZMNiDUFJBTUIS7F1%2F 38VwLd8%3D&RelayState=h ttps%3A%2F%2Fwww.googl e.com%2Fa%2Fnyu.edu%2F ServiceLogin%3Fservice%3D mail%26passive%3Dtrue%2 6rm%3Dfalse%26continue% 3Dhttps%253A%252F%252F mail.google.com%252Fmail %252F%26ss%3D1%26ltmpl %3Ddefault%26ltmplcache% 3D2%26emr%3D1%26osid% 3D1, 302, https://shibboleth.nyu.edu/id p/profile/SAML2/Redirect/SS O?execution=e1s1	3/2/2020, 8:15:01 PM

Evidence : frame-ancestors 'none';

nyu.edu	http://cs.nyu.edu/	https://cs.nyu.edu/	http://cs.nyu.edu/, 301, https://cs.nyu.edu/	3/2/2020, 8:10:33 PM
---------	--------------------	---------------------	---	----------------------

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
Evidence : upgrade-insecure-requests				

## !! Website does not implement X-XSS-Protection Best Practices

-0.3 SCORE IMPACT

Not explicitly setting X-XSS-Protection means that clients viewing a website could be at risk of reflected Cross-site Scripting (XSS) attacks.

### Description

The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when websites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP. Without these protections, an attacker can send their victims malicious URLs that inject code into the website

### Recommendation

Add the following header to responses from this website: 'X-XSS-Protection: 1; mode=block'

## 26 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&ltmpl=default&ltmplcache=2&emr=1&osid=1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVLJTsMwEL0j8Q%2BW71kahlsSJqiAEJVYojblwM0448SVYweP3cLfK6atCge4Pr95y3im15%2BdJhtwqKzJ6SROKQEjbK1Mk9NVdR9d0evi%2FGyKvNM9mwXfmgV8BEBPhkmDbHzlaXCGWY4KmeEdlPOCLWdPjyyLU9Y7662wmpL5XU6NFLqFvpG6U807rAVIYaVW%2FVqJWigldS3XLW8pet3Gynax5ogB5gY9N36	Header missing	3/2/2020, 8:15:01 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
			A0iyN0osozaosZZOUX Vy%2BUVlenG6U2Tf4L 9b7noTsoarKqHxZVqP ARtXgngd2ThtGw2xs N3OvuSlajPAkmsESma I4PwQ8NYaDB24JbiNE rBaPOa09b5HlITb7TY %2BySQ8MV8hhjokXC AtxrWysZn7sc%2F%2Fc %2FOjLy1OytPkhlRx%2 BK5di%2FlabUSX2S mtd3eOub%2BqOBdg BrcW9dx%2F7fbJJ6Mi KojOVJZMniDUFJBTUI S7F1%2F38VwLd8%3D &RelayState=https%3A %2F%2Fwww.google.c om%2Fa%2Fnyu.edu% 2FServiceLogin%3Fser vice%3Dmail%26passiv e%3Dtrue%26rm%3Dfa lse%26continue%3Dhtt ps%253A%252F%252F mail.google.com%252 Fmail%252F%26ss%3D 1%26ltmpl%3Ddefault% 26ltmplcache%3D2%2 6emr%3D1%26osid%3 D1, 302, <a href="https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1">https://shibboleth.nyu.edu/idp/profile/SAML2/R edirect/SSO? execution=e1s1</a>		

Evidence :

nyuwireless.org	<a href="http://calendar.nyuwireless.org/">http://calendar.nyuwireless.org/</a>	<a href="https://calendar.nyuwireless.org/">https://calendar.nyuwireless.org/</a>	http://calendar.nyuwireless.org/, 302, <a href="https://calendar.nyuwireless.org/">https://calendar.nyuwireless.org/</a>	Header missing	3/2/2020, 8:15:00 PM
-----------------	---	---	---	----------------	----------------------

Evidence :

nyuwireless.org	<a href="https://files.nyuwireless.org/">https://files.nyuwireless.org/</a>	<a href="https://files.nyuwireless.org/">https://files.nyuwireless.org/</a>	n/a	Header missing	3/2/2020, 8:14:58 PM
-----------------	---	---	-----	----------------	----------------------

Evidence :

nyuwireless.org	<a href="http://files.nyuwireless.org/">http://files.nyuwireless.org/</a>	<a href="http://files.nyuwireless.org/">http://files.nyuwireless.org/</a>	n/a	Header missing	3/2/2020, 8:14:58 PM
-----------------	---	---	-----	----------------	----------------------

Evidence :

nyuwireless.org	<a href="http://www.nyuwireless.org/">http://www.nyuwireless.org/</a>	<a href="https://wireless.engineering.nyu.edu/">https://wireless.engineering.nyu.edu/</a>	http://www.nyuwireless.org/, 301, <a href="http://nyuwireless.com">http://nyuwireless.com</a> , 301, <a href="https://wireless.engineering.nyu.edu/">https://wireless.engineering.nyu.edu/</a>	Header missing	3/2/2020, 8:14:58 PM
-----------------	---	---	---	----------------	----------------------

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
nyuwireless.org	http://ftp.nyuwireless.org/	http://ftp.nyuwireless.org/	n/a	Header missing	3/2/2020, 8:14:58 PM
Evidence :					
livewellnyu.org	https://www.livewellnyu.org/	https://collegehealthqi.nyu.edu/	https://www.livewellnyu.org/, 301, https://collegehealthqi.nyu.edu/	Header missing	3/2/2020, 8:14:57 PM
Evidence :					
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	Header missing	3/2/2020, 8:14:53 PM
Evidence :					
gonyuad.com	https://www.gonyuad.com/	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/index, 302, https://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:52 PM
Evidence :					
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:50 PM
Evidence :					
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	Header missing	3/2/2020, 8:14:47 PM
Evidence :					
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	Header missing	3/2/2020, 8:14:46 PM
Evidence :					
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	Header missing	3/2/2020, 8:14:44 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	Header missing	3/2/2020, 8:14:40 PM
Evidence :					
nyu.edu	http://archive.nyu.edu/	https://archive.nyu.edu/	http://archive.nyu.edu/, 302, https://archive.nyu.edu/	Header missing	3/2/2020, 8:10:38 PM
Evidence :					
nyu.edu	http://m.nyu.edu/	https://m.nyu.edu/default/nyu_app_index/index	http://m.nyu.edu/, 301, https://m.nyu.edu/, 302, https://m.nyu.edu/default/nyu_app_index/index	Header missing	3/2/2020, 8:10:36 PM
Evidence :					
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	Header missing	3/2/2020, 8:10:35 PM
Evidence :					
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	http://login.nyu.edu/	https://login.nyu.edu/	http://login.nyu.edu/, 302, https://login.nyu.edu/	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
nyu.edu	http://cs.nyu.edu/	https://cs.nyu.edu/	http://cs.nyu.edu/, 301, https://cs.nyu.edu/	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	Header missing	3/2/2020, 8:10:32 PM
Evidence :					

## ✓ Web Application Firewall (WAF) Detected

A web application firewall (WAF) monitors traffic to and from a web application, and attempts to detect and block traffic associated with common malicious behaviors. A WAF is an important defensive layer that helps secure your web application.

### Description

A well configured WAF can detect and block a wide variety of attacks. Capabilities vary between products, but at minimum most WAFs can block SQL injection and Cross Site Scripting attacks. A WAF is no substitute to a well-designed web application that is not vulnerable to these attacks in the first place, but it still plays an important role in providing layered security.

### Recommendation

Companies should consider implementing a web application firewall that can protect against common web vulnerabilities, such as SQL Injection and cross-site scripting (XSS). Many hosting providers offer WAF capabilities as well.

## 16 findings

DOMAIN	URL	LAST OBSERVED
nyu.edu	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	3/2/2020, 8:15:01 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyuonline.com	http://www.nyu.edu	3/2/2020, 8:15:01 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyujade.org	https://www.nyujade.org/	3/2/2020, 8:14:59 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyujade.org	http://www.nyujade.org/	3/2/2020, 8:14:59 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyubraces.com	http://dental.nyu.edu/patientcare/orthodontics_patients.html	3/2/2020, 8:14:54 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	URL	LAST OBSERVED
nyucareers.com	https://www.nyucareers.com/	3/2/2020, 8:14:49 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyujade.org	https://nyujade.org/	3/2/2020, 8:14:49 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyujade.org	http://nyujade.org/	3/2/2020, 8:14:48 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
gonyuathletics.com	https://gonyuathletics.merchorders.com	3/2/2020, 8:14:47 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyucareers.com	https://nyucareers.com/	3/2/2020, 8:14:39 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	https://auth.nyu.edu/authenticationendpoint/index.jsp	3/2/2020, 8:10:34 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	http://beta.nyu.edu/	3/2/2020, 8:10:34 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	https://login.nyu.edu/	3/2/2020, 8:10:34 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	http://admissions.nyu.edu/	3/2/2020, 8:10:33 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	https://beta.nyu.edu/	3/2/2020, 8:10:33 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		
nyu.edu	https://www.nyu.edu/	3/2/2020, 8:10:15 PM
Evidence : F5 BIG-IP LTM detected with 25% confidence.		

## !! Redirect Chain Contains HTTP

-0.5 SCORE IMPACT

Site redirects through URLs that are not secured with HTTPS; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the intended destination site.

### Description

While redirecting a user to their ultimate URL destination, the user passes through one or more URLs served over HTTP (instead of HTTPS). Having HTTP links in a redirect chain

### Recommendation

Any HTTP site should immediately redirect users to HTTPS-protected URLs and ensure that any further redirects do not occur over HTTP. Prefer the usage of HTTPS URLs over HTTP when available, avoiding an unnecessary redirect.

weakens other security technologies (e.g., HTTPS and HSTS headers) that are deployed elsewhere in the chain.

#### 4 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	3/2/2020, 8:14:58 PM
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	3/2/2020, 8:14:50 PM
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin? service=mail&passive=true& rm=false&continue=https://mail.google.com/mail/&ss=1&lt mpl=default&ltmplcache=2& emr=1&osid=1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO? SAMLRequest=fVLJTsMwEL 0j8Q%2BW71kahISsJqiAEJV YojblwM0448SVYweP3cLfk6 atCge4Pr95y3im15%2BdJht wqKzJ6SROKQEjbK1Mk9NV dR9d0evi%2FGyKvNM9mwX fmgV8BEBPhkmDbHzlaXCG WY4KmeEdlPOCLWdPjyyLU 9Y7662wmpL5XU6NFLqFvp G6U807rAVIYaVW%2FVqJW igldS3XLW8peT3Gynax5ogB 5gY9N36A0iyN0osozaosZZ OUXVvy%2BUVlenG6U2Tf4L 9b7noTsoarKqHxZVqPARtXg ngd2ThtrGw2xsN3OvuSlajP AkmsESmal4PwQ8NYaDB2 4JbiNErBaPOa09b5HliTb7T Y%2BySQ8MV8hhjokXCAtxr WysZh7sc%2F%2Fc%2FOjLy1 OytPkh1Rx%2BK5di%2Flab USX2Smtd3eOuB%2BqOBd GBrcW9dx%2F7fbJJ6MiKoj OVJZMNiDUFJBTUIS7F1%2F 38VwlD8%3D&RelayState=h ttps%3A%2F%2Fwww.googl e.com%2Fa%2Fnnyu.edu%2F ServiceLogin%3Fservice%3D mail%26passive%3Dtrue%2 6rm%3Dfalse%26continue% 3Dhttps%253A%252F%252F mail.google.com%252Fmail %252F%26ss%3D1%26ltmpl %3Ddefault%26ltmplcache% 3D2%26emr%3D1%26osid% 3D1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	3/2/2020, 8:10:35 PM

## i Website References Object Storage

Objects (files) stored in object storage buckets (storage partitions) can be downloaded, referenced, and used by websites.

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

**Description**

There is no risk in using object storage services in this fashion. However, if the Access Control List (ACL) on the bucket (storage partition) the website is hosted on is misconfigured, then the website may be compromised or defaced by attackers.

**Recommendation**

Ensure that the usage of external services, such as Amazon S3, conforms to company policies.

**6 findings**

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:14:46 PM
Evidence : s3.amazonaws.com/assets.sidearmsports.com					
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:10:34 PM
Evidence : s3.amazonaws.com/nyu.edu					
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:10:34 PM
Evidence : s3.amazonaws.com/nyulibraries-www-assets					
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:10:33 PM
Evidence : s3.amazonaws.com/nyu.edu					
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:10:33 PM
Evidence : s3.amazonaws.com/nyu.edu					
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	HTTP response body references an Amazon S3 bucket	3/2/2020, 8:10:32 PM
Evidence : s3.amazonaws.com/nyulibraries-www-assets					

**i Content Security Policy (CSP) Missing**

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

**Description**

The Content Security Policy provides a valuable safety net that protects your website from malicious cross-site scripting (XSS) attacks. A well configured policy will stop an attacker attempting to inject their code, or references to other malicious

**Recommendation**

Enable CSP headers via your webserver configuration.

content, into your website. Without a Content Security Policy, it's easy for website developers to make mistakes that allow an attacker to inject content that changes the way the website behaves.

## 26 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyuwireless.org	http://calendar.nyuwireless.org/	https://calendar.nyuwireless.org/	http://calendar.nyuwireless.org/, 302, https://calendar.nyuwireless.org/	3/2/2020, 8:15:00 PM
Evidence : No content security policy directives found.				
nyuwireless.org	https://files.nyuwireless.org/	https://files.nyuwireless.org/	n/a	3/2/2020, 8:14:58 PM
Evidence : No content security policy directives found.				
nyuwireless.org	http://files.nyuwireless.org/	http://files.nyuwireless.org/	n/a	3/2/2020, 8:14:58 PM
Evidence : No content security policy directives found.				
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	3/2/2020, 8:14:58 PM
Evidence : No content security policy directives found.				
nyuwireless.org	http://ftp.nyuwireless.org/	http://ftp.nyuwireless.org/	n/a	3/2/2020, 8:14:58 PM
Evidence : No content security policy directives found.				
livewellnyu.org	https://www.livewellnyu.org/	https://collegehealthqi.nyu.edu/	https://www.livewellnyu.org/, 301, https://collegehealthqi.nyu.edu/	3/2/2020, 8:14:57 PM
Evidence : No content security policy directives found.				
wnyu.org	https://www.wnyu.org/	https://www.wnyu.org/	n/a	3/2/2020, 8:14:54 PM
Evidence : No content security policy directives found.				
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	3/2/2020, 8:14:53 PM
Evidence : No content security policy directives found.				

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
gonyuad.com	https://www.gonyuad.com/	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/index, 302, https://www.gonyuad.com/landing/index	3/2/2020, 8:14:52 PM
Evidence : No content security policy directives found.				
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	3/2/2020, 8:14:50 PM
Evidence : No content security policy directives found.				
nyualumni.com	https://video.nyualumni.com/	http://video.alumni.nyu.edu	https://video.nyualumni.com/, 302, http://video.alumni.nyu.edu	3/2/2020, 8:14:48 PM
Evidence : No content security policy directives found.				
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	3/2/2020, 8:14:47 PM
Evidence : No content security policy directives found.				
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	3/2/2020, 8:14:46 PM
Evidence : No content security policy directives found.				
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	3/2/2020, 8:14:44 PM
Evidence : No content security policy directives found.				
wnyu.org	https://wnyu.org/	https://wnyu.org/	n/a	3/2/2020, 8:14:43 PM
Evidence : No content security policy directives found.				
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM
Evidence : No content security policy directives found.				

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM
Evidence : No content security policy directives found.				
nyu.edu	http://archive.nyu.edu/	https://archive.nyu.edu/	http://archive.nyu.edu/, 302, https://archive.nyu.edu/	3/2/2020, 8:10:38 PM
Evidence : No content security policy directives found.				
nyu.edu	http://m.nyu.edu/	https://m.nyu.edu/default/nyu_app_index/index	http://m.nyu.edu/, 301, https://m.nyu.edu/, 302, https://m.nyu.edu/default/nyu_app_index/index	3/2/2020, 8:10:36 PM
Evidence : No content security policy directives found.				
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	3/2/2020, 8:10:35 PM
Evidence : No content security policy directives found.				
nyu.edu	https://auth.nyu.edu/	https://auth.nyu.edu/authenticationendpoint/index.jsp	https://auth.nyu.edu/, 302, https://auth.nyu.edu/carbon, 302, https://auth.nyu.edu/carbon/admin/index.jsp, 302, https://auth.nyu.edu/carbon/admin/login.jsp, 302, https://auth.nyu.edu/authenticationendpoint/index.jsp	3/2/2020, 8:10:34 PM
Evidence : No content security policy directives found.				
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	3/2/2020, 8:10:34 PM
Evidence : No content security policy directives found.				
nyu.edu	http://login.nyu.edu/	https://login.nyu.edu/	http://login.nyu.edu/, 302, https://login.nyu.edu/	3/2/2020, 8:10:34 PM
Evidence : No content security policy directives found.				
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	3/2/2020, 8:10:33 PM
Evidence : No content security policy directives found.				
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	3/2/2020, 8:10:33 PM
Evidence : No content security policy directives found.				
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	3/2/2020, 8:10:33 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
Evidence : No content security policy directives found.				

## i Content Security Policy Contains 'unsafe-\*' Directive

A Content Security Policy (CSP) directive tells a web browser what locations it can load resources from when rendering a webpage. This helps prevent mistaken or malicious resources from being injected into a webpage (and then executed by a user's browser).

### Description

The Content Security Policy (CSP) header can mitigate Cross-Site Scripting (XSS) attacks by prohibiting the browser from running code embedded within the HTML of your site. However, the use of unsafe-eval and unsafe-inline policies in the CSP prevent this key safety feature from functioning. These unsafe directives mean that, should the site be vulnerable to XSS or HTML injection attacks, the attacker will be able to inject their own resources directly into the HTML response and have the browser execute them.

### Recommendation

Remove the unsafe directives from the content security policy. For trusted resources that must be used inline with HTML, you can use nonces or hashes in your content security policy's source list to mark the resources as trusted. Nonces are randomly generated numbers placed with inline content that you trust. By including the nonce in both the content and the header, the browser knows to trust the script. Example inline script with a nonce: <script nonce=aBFef03ncelOfn39hr3rsatsdfa>alert('Hello, world.');

</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'nonce-aBFef03ncelOfn39hr3rsatsdfa' Warning: For nonces to be effective, they must be randomly regenerated every time the page is loaded. If an attacker can guess the nonce value, the protection is useless. Hashes work similarly to nonces, but only need to be generated once. By taking the hash of a script and including it in the header, it will mark the script as trusted. If the attacker tries to change the script, the hash will change and it will no longer be trusted. Example inline script to be hashed: <script>alert('Hello, world.');//</script> Example policy that allows the inline script to be run without unsafe directives: Content-Security-Policy: script-src 'sha256-qznLcsROx4GACP2dm0UCKCzCG-HiZ1guq6ZZDob\_Tng='

### 2 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	3/2/2020, 8:10:34 PM
			Evidence : default-src 'self' libraryh3lp.com *.libraryh3lp.com *.swiftpcdn.com *.swiftype.com lgapi.libapps.com nyulibraries.statuspage.io app.library.nyu.edu;script-src 'self' 'unsafe-eval' 'unsafe-inline' libraryh3lp.com *.libraryh3lp.com *.googleapis.com maps.gstatic.com api3.libcal.com lgapi-us.libapps.com webdev3.library.nyu.edu web1.library.nyu.edu cdn.library.nyu.edu secure.gaug.es *.swiftpcdn.com *.swiftype.com www.googletagmanager.com www.google-analytics.com api2.libanswers.com lgapi.libapps.com maxcdn.bootstrapcdn.com *.cloudfront.net;img-src * data:style-src 'self' 'unsafe-inline' fonts.googleapis.com cloud.typography.com www.nyu.edu webdev3.library.nyu.edu web1.library.nyu.edu cdn.library.nyu.edu *.swiftpcdn.com lgapi.libapps.com maxcdn.bootstrapcdn.com;frame-src 'self' *.qualtrics.com libraryh3lp.com *.libraryh3lp.com *.library.nyu.edu library.nyu.edu www.googletagmanager.com;font-src 'self' data: fonts.gstatic.com maxcdn.bootstrapcdn.com s.swiftpcdn.com sa.swiftpcdn.com	
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	3/2/2020, 8:10:32 PM
			Evidence : default-src 'self' libraryh3lp.com *.libraryh3lp.com *.swiftpcdn.com *.swiftype.com lgapi.libapps.com nyulibraries.statuspage.io app.library.nyu.edu;script-src 'self' 'unsafe-eval' 'unsafe-inline' libraryh3lp.com *.libraryh3lp.com *.googleapis.com maps.gstatic.com api3.libcal.com lgapi-us.libapps.com webdev3.library.nyu.edu web1.library.nyu.edu cdn.library.nyu.edu secure.gaug.es *.swiftpcdn.com *.swiftype.com www.googletagmanager.com www.google-analytics.com api2.libanswers.com lgapi.libapps.com maxcdn.bootstrapcdn.com *.cloudfront.net;img-src * data:style-src 'self' 'unsafe-inline' fonts.googleapis.com cloud.typography.com www.nyu.edu webdev3.library.nyu.edu web1.library.nyu.edu cdn.library.nyu.edu *.swiftpcdn.com lgapi.libapps.com maxcdn.bootstrapcdn.com;frame-src 'self' *.qualtrics.com libraryh3lp.com *.libraryh3lp.com *.library.nyu.edu library.nyu.edu www.googletagmanager.com;font-src 'self' data: fonts.gstatic.com maxcdn.bootstrapcdn.com s.swiftpcdn.com sa.swiftpcdn.com	

## !! Website Does Not Implement HSTS Best Practices

-0.5 SCORE IMPACT

Even if a website is protected with HTTPS, most browsers will still try first to connect to the HTTP version of the website unless explicitly specified. At that moment, visitors to the website are vulnerable to a man-in-the-middle attacker that can prevent them from reaching the HTTPS version of the website they intended to visit and instead divert them to a malicious website. The (expand) HSTS header ensures that, after a user's initial visit to the website, that they will not be susceptible to this man-in-the-middle attack because they will immediately connect to the HTTPS-protected website.

## Description

HTTP Strict Transport Security is an HTTP header that instructs clients (e.g., web browsers) to only connect to a website over encrypted HTTPS connections. Clients that respect this header will automatically upgrade all connection attempts from HTTP to HTTPS. After a client receives the HSTS header upon its first website visit, future connections to that website are protected against Man-in-the-Middle attacks that attempt to downgrade to an unencrypted HTTP connection. The browser will expire the HTTP Strict Transport Security header after the number of seconds configured in the max-age attribute.

## Recommendation

Every web application (and any URLs traversed to arrive at the website via redirects) should set the HSTS header to remain in effect for at least 12 months (31536000 seconds). It is also recommended to set the 'includeSubDomains' directive so that requests to subdomains are also automatically upgraded to HTTPS. An acceptable HSTS header would declare: Strict-Transport-Security: max-age=31536000; includeSubDomains;

## 34 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&ltmpl=default&ltmplcache=2&emr=1&osid=1, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVLJTsMwEL0j8Q%2BW71kahISsJqiAEJVYojblwM0448SVYweP3cLfk6atCge4Pr95y3im15%2BdJhtwqKzJ6SROKQEjbK1Mk9NVdR9d0evi%2FGyKvNM9mwXfrmV8BEBPhkmDbHzlaXCGWY4KmeEdlPOCLWdPjyyLU9Y7662wmpL5XU6NFLqFvpG6U807rAVIYaVW%2FVqJWigldS3XLW8peT3Gynax5ogB5gY9N36A0iyN0osozaosZZOUXVy%2BUVlenG6U2Tf4L9b7noTsoarKqHxZVqPARtXgngd2ThtrGw2xs	Header missing includeSubDomains directive	3/2/2020, 8:15:01 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
			N3OvuSlajPAkmsESma I4PwQ8NYaDB24JbiNE rBaPOa09b5HliTb7TY %2BySQ8MV8hhjokXC AtxrWysZn7sc%2F%2Fc %2FOjly1OytPkhh1Rx%2 BK5di%2FdabUSX2S mtd3eOub%2BqOBdG BrcW9dx%2F7fbJJ6Mi KojOVJZMNiDUFJBTUI S7F1%2F38VwLd8%3D &RelayState=https%3A %2F%2Fwww.google.c om%2Fa%2Fnyu.edu% 2FServiceLogin%3Fser vice%3Dmail%26passiv e%3Dtrue%26rm%3Dfa lse%26continue%3Dhtt ps%253A%252F%252F mail.google.com%252 Fmail%252F%26ss%3D 1%26ltmpl%3Ddefault% 26ltmplcache%3D2%2 6emr%3D1%26osid%3 D1, 302, <a href="https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1">https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1</a>		

Evidence : Strict-Transport-Security: max-age=0

nyu.edu	http://mail.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://mail.nyu.edu/, 301, http://email.nyu.edu/, 301, http://mail.google.com/a/nyu.edu, 302, https://mail.google.com/a/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin? service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&ltmpl=default&ltmplcache=2&emr=1&osid=1, 302, <a href="https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVLJTsmwEL0j8Q%2BW71kahlsJqiAEJVYojblwM0448SVYweP3cLf6atCge4Pr95y3im15%2BdJhtwqKzJ6SROKQEjbK1Mk9NVdR9d0evi%2FGyKvNM9mwXfmgV8BEBPhkmDbHzlaXCGWY4Kme">https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVLJTsmwEL0j8Q%2BW71kahlsJqiAEJVYojblwM0448SVYweP3cLf6atCge4Pr95y3im15%2BdJhtwqKzJ6SROKQEjbK1Mk9NVdR9d0evi%2FGyKvNM9mwXfmgV8BEBPhkmDbHzlaXCGWY4Kme</a>	Max-age is shorter than best practices	3/2/2020, 8:15:01 PM
---------	----------------------	--	---	--	----------------------

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
			EdIPOCLWdPjyyLU9Y7 662wmpL5XU6NFLqFv pG6U807rAVIYaVW%2 FVqJWigldS3XLW8peT 3Gynax5ogB5gY9N36 AOiyN0osozaosZZOUX Vy%2BUVlenG6U2Tf4L 9b7noTsoarKqHxZVqP ARTXgngd2ThtrGw2xs N3OvuSlajPAkmsESma I4PwQ8NYaDB24JbiNE rBaPOa09b5HlITb7TY %2BySQ8MV8hhjokXC AtxrWysZn7sc%2F%2Fc %2FOjLy1OytPkhlRx%2 BK5di%2FlabUSX2S mtd3eOuB%2BqOBdG BrcW9dx%2F7fbJJ6Mi KoJOVJZMNiDUFJBTUI S7F1%2F38VwLd8%3D &RelayState=https%3A %2F%2Fwww.google.c om%2Fa%2Fnyu.edu% 2FServiceLogin%3Fser vice%3Dmail%26passiv e%3Dtrue%26rm%3Dfa lse%26continue%3Dhtt ps%253A%252F%252F mail.google.com%252 Fmail%252F%26ss%3D 1%26ltmpl%3Ddefault% 26ltmplcache%3D2%2 6emr%3D1%26osid%3 D1, 302, <a href="https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1">https://shibboleth.nyu.edu/idp/profile/SAML2/R edirect/SSO? execution=e1s1</a>		
Evidence : Strict-Transport-Security: max-age=0					
nyuwireless.org	<a href="http://calendar.nyuwireless.org/">http://calendar.nyuwireless.org/</a>	<a href="https://calendar.nyuwireless.org/">https://calendar.nyuwireless.org/</a>	http://calendar.nyuwireless.org/, 302, <a href="https://calendar.nyuwireless.org/">https://calendar.nyuwireless.org/</a>	No HSTS header found	3/2/2020, 8:15:00 PM
Evidence :					
nyujade.org	<a href="https://www.nyujade.org/">https://www.nyujade.org/</a>	<a href="https://www.nyujade.org/">https://www.nyujade.org/</a>	n/a	No HSTS header found	3/2/2020, 8:14:59 PM
Evidence :					
nyuwireless.org	<a href="https://files.nyuwireless.org/">https://files.nyuwireless.org/</a>	<a href="https://files.nyuwireless.org/">https://files.nyuwireless.org/</a>	n/a	No HSTS header found	3/2/2020, 8:14:58 PM
Evidence :					

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	No HSTS header found	3/2/2020, 8:14:58 PM
Evidence :					
livewellnyu.org	https://www.livewellnyu.org/	https://collegehealthqi.nyu.edu/	https://www.livewellnyu.org/, 301, https://collegehealthqi.nyu.edu/	No HSTS header found	3/2/2020, 8:14:57 PM
Evidence :					
wnyu.org	https://www.wnyu.org/	https://www.wnyu.org/	n/a	No HSTS header found	3/2/2020, 8:14:54 PM
Evidence :					
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	No HSTS header found	3/2/2020, 8:14:53 PM
Evidence :					
nyuad-artscenter.org	http://cms.nyuad-artscenter.org/	https://cms.nyuad-artscenter.org/	http://cms.nyuad-artscenter.org/, 302, https://cms.nyuad-artscenter.org/	No HSTS header found	3/2/2020, 8:14:52 PM
Evidence :					
gonyuad.com	https://www.gonyuad.com/	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/index, 302, https://www.gonyuad.com/landing/index	No HSTS header found	3/2/2020, 8:14:52 PM
Evidence :					
nyucareers.com	https://www.nyucareers.com/	https://www.nyucareers.com/	n/a	Header missing includeSubDomains directive	3/2/2020, 8:14:49 PM
Evidence : Strict-Transport-Security: max-age=86400					
nyucareers.com	https://www.nyucareers.com/	https://www.nyucareers.com/	n/a	Max-age is shorter than best practices	3/2/2020, 8:14:49 PM
Evidence : Strict-Transport-Security: max-age=86400					
nyujade.org	https://nyujade.org/	https://nyujade.org/	n/a	No HSTS header found	3/2/2020, 8:14:49 PM
Evidence :					

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	No HSTS header found	3/2/2020, 8:14:47 PM
Evidence :					
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	No HSTS header found	3/2/2020, 8:14:46 PM
Evidence :					
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	No HSTS header found	3/2/2020, 8:14:44 PM
Evidence :					
wnyu.org	https://wnyu.org/	https://wnyu.org/	n/a	No HSTS header found	3/2/2020, 8:14:43 PM
Evidence :					
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	No HSTS header found	3/2/2020, 8:14:40 PM
Evidence :					
nyucareers.com	https://nyucareers.com/	https://nyucareers.com/	n/a	Header missing includeSubDomains directive	3/2/2020, 8:14:39 PM
Evidence : Strict-Transport-Security: max-age=86400					
nyucareers.com	https://nyucareers.com/	https://nyucareers.com/	n/a	Max-age is shorter than best practices	3/2/2020, 8:14:39 PM
Evidence : Strict-Transport-Security: max-age=86400					
nyu.edu	http://archive.nyu.edu/	https://archive.nyu.edu/	http://archive.nyu.edu/, 302, https://archive.nyu.edu/	No HSTS header found	3/2/2020, 8:10:38 PM
Evidence :					
nyu.edu	http://m.nyu.edu/	https://m.nyu.edu/default/nyu_app_index/index	http://m.nyu.edu/, 301, https://m.nyu.edu/, 302, https://m.nyu.edu/default/nyu_app_index/index	Header missing includeSubDomains directive	3/2/2020, 8:10:36 PM
Evidence : Strict-Transport-Security: max-age=31536000;					

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	No HSTS header found	3/2/2020, 8:10:35 PM
Evidence :					
nyu.edu	https://auth.nyu.edu/	https://auth.nyu.edu/authenticationendpoint/index.jsp	https://auth.nyu.edu/, 302, https://auth.nyu.edu/carbon, 302, https://auth.nyu.edu/carbon/admin/index.jsp, 302, https://auth.nyu.edu/carbon/admin/login.jsp, 302, https://auth.nyu.edu/authenticationendpoint/index.jsp	No HSTS header found	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	No HSTS header found	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	http://login.nyu.edu/	https://login.nyu.edu/	http://login.nyu.edu/, 302, https://login.nyu.edu/	No HSTS header found	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	Header missing includeSubDomains directive	3/2/2020, 8:10:34 PM
Evidence : Strict-Transport-Security: max-age=31536000					
nyu.edu	https://adminpublic.nyu.edu/	https://adminpublic.nyu.edu/	n/a	No HSTS header found	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	No HSTS header found	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	http://cs.nyu.edu/	https://cs.nyu.edu/	http://cs.nyu.edu/, 301, https://cs.nyu.edu/	No HSTS header found	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	No HSTS header found	3/2/2020, 8:10:33 PM
Evidence :					
nyu.edu	https://beta.nyu.edu/	https://beta.nyu.edu/	n/a	No HSTS header found	3/2/2020, 8:10:33 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
nyu.edu	https://nyu.edu/	https://www.nyu.edu/	https://nyu.edu/, 302, https://www.nyu.edu/	No HSTS header found	3/2/2020, 8:10:15 PM
Evidence :					

## i Unsafe Implementation Of Subresource Integrity

Subresource integrity (SRI) is a security feature that enables browsers to verify that files they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing website elements to provide a cryptographic hash that a fetched file must match.

### Description

Many websites that rely on JavaScript and CSS stylesheet files will host these static resources with external organizations (typically CDNs) to improve website load times. Unfortunately, if one of these external organizations is compromised then the JavaScript and CSS files it hosts can also be compromised and used to push malicious code to the original website. Subresource integrity is a way for a website owner to add a checksum value to all externally-hosted files that is used by the browser to verify that files loaded from external organizations have not been modified.

### Recommendation

Please ensure that all website elements (i.e. `<script>` and `<link>`) loading JavaScript and CSS stylesheets hosted with external organizations contain the 'integrity' directive with a valid checksum. Example: `<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8Kuxy9rx7HNQIGYI1kPzQh01wx4JwY8wC" crossorigin="anonymous"></script>`

### 17 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
Evidence : <script type="text/javascript" src="https://vr2.verticalresponse.com/signup_forms/signup_forms.embedded-2.js"><link rel="stylesheet" id="nyu-wireless-google-fonts-css" href="https://fonts.googleapis.com/css?family=Lato%3A400%2C400italic%2C700%2C300italic%2C300%2C700italic&ver=4.9.8" type="text/css" media="all"><link rel="stylesheet" id="nyu-wireless-font-awesome-css" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css?ver=4.9.8" type="text/css" media="all">				
nyuwireless.org	http://www.nyuwireless.org/	https://wireless.engineering.nyu.edu/	http://www.nyuwireless.org/, 301, http://nyuwireless.com, 301, https://wireless.engineering.nyu.edu/	3/2/2020, 8:14:58 PM
Evidence : <script src="//use.typekit.net/kon0mpg.js"><script src="//ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"><script type="text/javascript" src="//s7.addthis.com/js/300/addthis_widget.js#pubid=ra-4f686dce243379ce&async=1">				
nyuad-artscenter.org	https://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	https://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	3/2/2020, 8:14:53 PM
Evidence : <script src="https://cdn.prestosports.com/action/cdn/info/jquery.js"><script src="https://cdn.prestosports.com/action/cdn/info/modernizr.js"><script type="text/javascript" src="https://cdn.prestosports.com/action/cdn/info/cookie-handler.js"><script data-main="https://cdn.prestosports.com/action/cdn/info/main.js" src="https://cdn.prestosports.com/action/cdn/info/vendor/require.js"><script type="text/javascript" src="//securepubads.g.doubleclick.net/tag/js/gpt.js">				
gonyuad.com	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/landing/index	https://www.gonyuad.com/, 302, https://www.gonyuad.com/landing, 302, https://www.gonyuad.com/landing/index	3/2/2020, 8:14:52 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	3/2/2020, 8:14:50 PM
<p>Evidence : &lt;script src="https://cdn.prestosports.com/action/cdn/info/jquery.js"&gt;&lt;script src="https://cdn.prestosports.com/action/cdn/info/modernizr.js"&gt;&lt;script type="text/javascript" src="https://cdn.prestosports.com/action/cdn/info/cookie-handler.js"&gt;&lt;script data-main="https://cdn.prestosports.com/action/cdn/info/main.js" src="https://cdn.prestosports.com/action/cdn/info/vendor/require.js"&gt;&lt;script type="text/javascript" src="//securepubads.g.doubleclick.net/tag/js/gpt.js"&gt;</p>				
nyualumni.com	https://video.nyualumni.com/	http://video.alumni.nyu.edu	https://video.nyualumni.com/, 302, http://video.alumni.nyu.edu	3/2/2020, 8:14:48 PM
<p>Evidence : &lt;script src="//players.brightcove.net/5446914890001/BJ40WY_MW_default/index.min.js"&gt;&lt;link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/714802/css/fonts.css"&gt;</p>				
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	3/2/2020, 8:14:47 PM
<p>Evidence : &lt;script type="text/javascript" src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js"&gt;&lt;script src="https://optanon.blob.core.windows.net/consent/77124b5b-94ec-4dec-b29a-6639e5c32d19.js" type="text/javascript" charset="UTF-8"&gt;&lt;link rel="stylesheet" href="//maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css"&gt;</p>				
gonyuathletics.com	https://www.gonyuathletics.com/	https://gonyuathletics.com/	https://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	3/2/2020, 8:14:46 PM
<p>Evidence : &lt;script type="text/javascript" src="https://cdnjs.cloudflare.com/ajax/libs/modernizr/2.8.3/modernizr.js"&gt;&lt;script src="//ajax.googleapis.com/ajax/libs/jquery/1.7.2/jquery.min.js" type="text/javascript"&gt;&lt;script src="https://cdnjs.cloudflare.com/ajax/libs/swfobject/2.2/swfobject.js" type="text/javascript"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/common/js/default/15/master_compressed_v5.js" type="text/javascript"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/common/js/msajax.js" type="text/javascript"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/plugins/jquery.jtweetsanywhere-1.3.1.min.js"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/plugins/jquery.mCustomScrollbar.js"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/plugins/jquery.overflow-2.0.js"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/responsive/js/accessibility-nogulp.1519400584000.js"&gt;&lt;script src="https://s3.amazonaws.com/assets.sidearmsports.com/responsive/js/default-accessibility.1564775762723.js"&gt;&lt;link type="text/css" rel="stylesheet" href="https://s3.amazonaws.com/assets.sidearmsports.com/common/css/default/5/core_compressed.css"&gt;&lt;link href="https://fonts.googleapis.com/css?family=Titillium+Web:400,600,700,900,300,400italic" rel="stylesheet" type="text/css"&gt;&lt;link href="https://fonts.sidearmsports.com/sidearm/sidearm_font.css" rel="stylesheet" type="text/css"&gt;</p>				
livewellnyu.com	http://livewellnyu.com/	https://livewellnyu.com/	http://livewellnyu.com/, 301, https://livewellnyu.com/	3/2/2020, 8:14:44 PM
<p>Evidence : &lt;script type="text/javascript" src="//connect.facebook.net/en_US/sdk.js#xfbml=1&amp;version=v2.4&amp;appId=374944666254868"&gt;&lt;link rel="stylesheet" id="googleFont-style-css" href="https://fonts.googleapis.com/css?family=Raleway%3A500%2C700&amp;ver=4.7.16" type="text/css" media="all"&gt;</p>				
gonyuad.com	https://gonyuad.com/	https://gonyuad.com/landing/index	https://gonyuad.com/, 302, https://gonyuad.com/index, 302, https://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM
<p>Evidence : &lt;script src="https://cdn.prestosports.com/action/cdn/info/jquery.js"&gt;&lt;script src="https://cdn.prestosports.com/action/cdn/info/modernizr.js"&gt;&lt;script type="text/javascript" src="https://cdn.prestosports.com/action/cdn/info/cookie-handler.js"&gt;&lt;script data-main="https://cdn.prestosports.com/action/cdn/info/main.js" src="https://cdn.prestosports.com/action/cdn/info/vendor/require.js"&gt;&lt;script type="text/javascript" src="//securepubads.g.doubleclick.net/tag/js/gpt.js"&gt;</p>				

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM
<p>Evidence : &lt;script src="https://cdn.prestosports.com/action/cdn/info/jquery.js"&gt;,&lt;script src="https://cdn.prestosports.com/action/cdn/info/modernizr.js"&gt;,&lt;script type="text/javascript" src="https://cdn.prestosports.com/action/cdn/info/cookie-handler.js"&gt;,&lt;script data-main="https://cdn.prestosports.com/action/cdn/info/main.js" src="https://cdn.prestosports.com/action/cdn/info/vendor/require.js"&gt;,&lt;script type="text/javascript" src="//securepubads.g.doubleclick.net/tag/js/gpt.js"&gt;</p>				
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	3/2/2020, 8:10:35 PM
<p>Evidence : &lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-includes/js/jquery/jquery.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__1.12.4-wp"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-includes/js/jquery/jquery-migrate.min.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__1.4.1"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/themes/astor-place/js/navigation.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180729" async=""&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/themes/astor-place/js/skip-link-focus-fix.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180729" defer=""&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/themes/astor-place/js scroll-effects.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180729"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/themes/astor-place/pluggable/lazyload/js/lazyload.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20151215" defer=""&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/plugins/subscribe-by-email/assets/js/widget.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/plugins/easy-fancybox/js/jquery.fancybox.min.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__1.3.24"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/plugins/easy-fancybox/js/jquery.easing.min.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__1.4.1"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/plugins/easy-fancybox/js/jquery.mousewheel.min.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__31.13"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-content/plugins/subscribe-by-email/assets/js/shortcode.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5"&gt;,&lt;script type="text/javascript" src="https://s18798.pcdn.co/wp-includes/js/wp-embed.min.js?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5"&gt;,&lt;link rel="stylesheet" id="wp-block-library-css" href="https://s18798.pcdn.co/wp-includes/css/dist/block-library/style.min.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="wp-components-css" href="https://s18798.pcdn.co/wp-includes/css/dist/components/style.min.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="wp-editor-font-css" href="https://fonts.googleapis.com/css?family=Noto+Serif%3A400%2C400%2C700%2C700i&amp;ver=5.2.5" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="wp-block-editor-css" href="https://s18798.pcdn.co/wp-includes/css/dist/block-editor/style.min.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="nyu_blocks-cgb-style-css" href="https://s18798.pcdn.co/wp-content/plugins/nyu-blocks/build(blocks.style.build.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__5.2.5)" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-fonts-css" href="https://fonts.googleapis.com/css?family=Montserrat%3A300%2C300%2C600%2C600&amp;subset=latin%2Clatin-ext" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-base-style-css" href="https://s18798.pcdn.co/wp-content/themes/astor-place/style.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180923" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-header-style-css" href="https://s18798.pcdn.co/wp-content/themes/astor-place/css/header.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180923" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-footer-style-css" href="https://s18798.pcdn.co/wp-content/themes/astor-place/css/footer.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180923" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-entry-style-css" href="https://s18798.pcdn.co/wp-content/themes/astor-place/css/entry.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180923" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="subscribe-by-email-widget-css" href="https://s18798.pcdn.co/wp-content/plugins/subscribe-by-email/assets/css/widget/widget.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20130522" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="fancybox-css" href="https://s18798.pcdn.co/wp-content/plugins/easy-fancybox/css/jquery.fancybox.min.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__13.24" type="text/css" media="screen"&gt;,&lt;link rel="stylesheet" id="sbe-form-css" href="https://s18798.pcdn.co/wp-content/plugins/subscribe-by-email/assets/css/shortcode.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20140212" type="text/css" media="all"&gt;,&lt;link rel="stylesheet" id="astorplace-content-css" href="https://s18798.pcdn.co/wp-content/themes/astor-place/css/content.css?ver=bd3bcfb9b8ae007984bd1e53c2a6e38e5d9406b__20180923" type="text/css" media="all"&gt;</p>				
nyu.edu	http://as.nyu.edu/	https://as.nyu.edu/	http://as.nyu.edu/, 302, https://as.nyu.edu/	3/2/2020, 8:10:34 PM
<p>Evidence : &lt;link rel="stylesheet" type="text/css" href="https://cloud.typography.com/7436432/7555752/css/fonts.css"&gt;</p>				
nyu.edu	https://library.nyu.edu/	https://library.nyu.edu/	n/a	3/2/2020, 8:10:34 PM
<p>Evidence : &lt;link rel="stylesheet" type="text/css" href="https://cloud.typography.com/7436432/789146/css/fonts.css"&gt;</p>				
nyu.edu	https://events.nyu.edu/	https://events.nyu.edu/	n/a	3/2/2020, 8:10:33 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
Evidence : <script type="text/javascript" src="https://maps-api-ssl.google.com/maps/api/js?v=3&key=AIzaSyDh8EsXAvvojd28ptX4IT7KslOlvUAozSw&sensor=false">,<script src="//s3.amazonaws.com/nyu.edu/globalnav/redesign/v1.0.3/global-nav.js"><link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/636084/css/fonts.css">,<link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/714802/css/fonts.css">,<link rel="stylesheet" href="https://s3.amazonaws.com/nyu.edu/globalnav/redesign/v1.0.3/global-nav.css">				
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	3/2/2020, 8:10:33 PM
Evidence : <script type="text/javascript" src="http://maps.googleapis.com/maps/api/js?key=AIzaSyDh8EsXAvvojd28ptX4IT7KslOlvUAozSw&sensor=false">,<script src="//s3.amazonaws.com/nyu.edu/globalnav/redesign/v1.0.3/global-nav.js"><link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/636084/css/fonts.css">,<link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/714802/css/fonts.css">,<link rel="stylesheet" href="https://s3.amazonaws.com/nyu.edu/globalnav/redesign/v1.0.3/global-nav.css">				
nyu.edu	https://bi.nyu.edu/	https://bi.nyu.edu/	n/a	3/2/2020, 8:10:33 PM
Evidence : <script async="" src="https://www.googletagmanager.com/gtag/js?id=UA-122965847-1">				
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	3/2/2020, 8:10:32 PM
Evidence : <link rel="stylesheet" type="text/css" href="//cloud.typography.com/7436432/789146/css/fonts.css">				

## !! Insecure HTTPS Redirect Pattern

-0.5 SCORE IMPACT

Site redirects to a domain in a way that limits the security provided by HTTPS and HTTP Strict Transport Security (HSTS) headers; this leaves users vulnerable to being redirected to a spoofed/ malicious version of the site.

### Description

The HTTP site redirects users to a new URL in a way that cannot be secured with HTTPS and HSTS headers. This leaves users open to man-in-the-middle attackers who can redirect them to a fraudulent/ spoofed version of the intended site. Please see “Site Does Not Enforce HTTPS” issue type for more information regarding man-in-the-middle scenarios.

### Recommendation

Any HTTP site should redirect the user to a secure (i.e. HTTPS) version of the same domain that was originally requested (or a higher-level/parent version of that same domain). For example, http://www.example.com should only redirect either to https://www.example.com or https://example.com. This redirect should be done before redirecting to any other domain or subdomain.

### 5 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
gonyuathletics.com	http://shop.gonyuathletics.com/	https://gonyuathletics.merchorders.com	http://shop.gonyuathletics.com/, 301, https://gonyuathletics.merchorders.com	Redirect goes to different apex domain	3/2/2020, 8:14:47 PM
Evidence :					
gonyuathletics.com	http://www.gonyuathletics.com/	https://gonyuathletics.com/	http://www.gonyuathletics.com/, 301, https://gonyuathletics.com/	Redirect does not include HSTS header	3/2/2020, 8:14:46 PM
Evidence :					
nyuad-artscenter.org	http://nyuad-artscenter.org/	https://www.nyuad-artscenter.org/	http://nyuad-artscenter.org/, 301, https://www.nyuad-artscenter.org/	Redirect goes to a different subdomain	3/2/2020, 8:14:42 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
Evidence :					
nyu.edu	http://blogs.nyu.edu/	https://wp.nyu.edu/	http://blogs.nyu.edu/, 301, https://wp.nyu.edu/	Redirect goes to a different subdomain	3/2/2020, 8:10:34 PM
Evidence :					
nyu.edu	http://calendar.nyu.edu/	https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1	http://calendar.nyu.edu/, 302, https://www.google.com/calendar/hosted/nyu.edu, 301, https://calendar.google.com/calendar/hosted/nyu.edu, 302, https://www.google.com/a/nyu.edu/ServiceLogin?service=cl&passive=1209600&osid=1&continue=https://calendar.google.com/calendar/render&followup=https://calendar.google.com/endar/render, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fVK7TsMwFN2R%2BAfLex4NDMhqggolUYIHRAMDm2vfnKaOHXztFv4eNwUBAx28HB%2Bfx%2FWdnr%2F3mmzAobKmpJMOpwSMsFKZVUmfmuvkjJ5Xx0dT5L0e2Cz4zjzCWwD0JL40yMaLkgZnmOWokBneAzlv2GJ2d8uKNGeDs94KqymZX5XUdv261e0aTKtaKbvXtV1L0%2FUrrqyWQzxCwXLglDx%2Fxyp2sealAeYGPTc%2BQnmRJ%2FIJkhdNkbNJzk5OXyipv5wulNk3OBRRuSchu2maOqkfFs0osFES3H1kl3RI7UpDKmy%2Fs685otpEuOUagZlZljgfa15ag6EHtwC3UQKeHm9L2nk%2FIMuy7Xab%2FshkPDmfIQUZMi6QVuNY2djM%2FZrn4dz825dWP8rT7JdU9fVduxbzq9pqJT7ITGu7vXTAfazgXYgNrq3ruf%2FfbZJORkTJpB2pLBgcQKhWgaQkq%2Fauf%2Fcibssn&RelayState=http%3A%2F%2Fwww.google.com%2Fa%2Fnyu.e	Redirect goes to different apex domain	3/2/2020, 8:10:34 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	ANALYSIS	LAST OBSERVED
			du%2FServiceLogin%3Fservice%3Dcl%26passive%3Dtrue%26osid%3D1%26continue%3Dhttps%253A%252F%252Fcalendar.google.com%252Fcalendar%252Frender%26followup%3Dhttps%253A%252F%252Fcalendar.google.com%252Fcalendar%252Frender, 302, https://shibboleth.nyu.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1		
Evidence :					

## !!! Site does not enforce HTTPS

-0.4 SCORE IMPACT

Site does not enforce the use of HTTPS encryption, leaving the user vulnerable to man-in-the-middle attackers (who can falsify data and inject malicious code).

### Description

The site responds to HTTP requests without ultimately redirecting the browser to a secure version of the page. Since the site allows plaintext traffic, a man-in-the-middle attacker is able to read and modify any information passed between the site and the user. There are a variety of situations in which an attacker can intercept plaintext traffic in a man-in-the-middle position, including but not limited to:

- \* Open Wi-Fi Hotspots
- \* WPA/WPA2 encrypted hot-spots where the attacker connected before the victim
- \* Malicious Wi-Fi access points
- \* Compromised switches and routers
- \* ARP poisoning on the same wired network

It's important to remember that in many of the above situations, an attacker can not only read traffic, but also actively modify the traffic. Even if a site that does not contain sensitive information, an attacker can still inject malicious content to a user's browser.

### Recommendation

Any site served to a user (possibly at the end of a redirect chain) should be served over HTTPS.

### 7 findings

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyuwireless.org	http://files.nyuwireless.org/	http://files.nyuwireless.org/	n/a	3/2/2020, 8:14:58 PM
nyuwireless.org	http://ftp.nyuwireless.org/	http://ftp.nyuwireless.org/	n/a	3/2/2020, 8:14:58 PM
gonyuad.com	http://www.gonyuad.com/	http://www.gonyuad.com/landing/index	http://www.gonyuad.com/, 302, http://www.gonyuad.com/index, 302, http://www.gonyuad.com/landing/index	3/2/2020, 8:14:50 PM

DOMAIN	INITIAL URL	FINAL URL	REQUEST CHAIN	LAST OBSERVED
nyualumni.com	https://video.nyualumni.com/	http://video.alumni.nyu.edu	https://video.nyualumni.com/, 302, http://video.alumni.nyu.edu	3/2/2020, 8:14:48 PM
gonyuad.com	http://gonyuad.com/	http://gonyuad.com/landing/index	http://gonyuad.com/, 302, http://gonyuad.com/index, 302, http://gonyuad.com/landing/index	3/2/2020, 8:14:40 PM
nyu.edu	http://events.nyu.edu/	http://events.nyu.edu/	n/a	3/2/2020, 8:10:33 PM
nyu.edu	http://library.nyu.edu/	http://library.nyu.edu/	n/a	3/2/2020, 8:10:32 PM

Security-related analyses, including ratings, and statements in the Content of this document 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. SECURITYSCORECARD 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 AND DEFECTS, (4) THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED AND (5) THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION.

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. © 2019 SecurityScorecard, Inc. All rights reserved.