Release Notes for Cisco Vulnerability Database (VDB) Update 340

About the Cisco Vulnerability Database

The Cisco vulnerability database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.

Cisco issues periodic updates to the VDB. The time it takes to update the VDB and its associated mappings on the Firepower Management Center depends on the number of hosts in your network map. As a rule of thumb, divide the number of hosts by 1000 to determine the approximate number of minutes to perform the update.

You can find VDB updates on the VDB Software Downloads page on Cisco.com.

About the Cisco Firepower Application Detector Reference

The *Cisco Firepower Application Detector Reference* contains the release notes and information about the application detectors supported in the VDB release. For each application listed in the reference, you can find the following information:

- Description—A brief description of the application.
- Categories—A general classification for the application that describes its most essential function. Example categories include web services provider, e-commerce, ad portal, and social networking.
- Tags—Predefined tags that provide additional information about the application. Example tags include webmail, SSL protocol, file sharing/transfer, and displays ads. An application can have zero, one, or more tags.
- Risk—The likelihood that the application is used for purposes that might be against your organization's security policy. The risk levels are Very High, High, Medium, Low, and Very Low.
- Business Relevance—The likelihood that the application is used within the context of your organization's business operations, as opposed to recreationally. The relevance levels are Very High, High, Medium, Low, and Very Low.

Supported Platforms and Software Versions

This guide relates to Vulnerability Database Updates installed via the following software versions on the following platforms:

Sourcefire 3D System/Firepower System Version 5.x:

- Cisco FireSIGHT Management Centers (formerly Defense Centers)

Firepower Version 6.x:

- Cisco Firepower Management Centers (formerly Defense Centers/FireSIGHT Management Centers)

Supported Detector Types

The following Detector Types are supported:

- application protocol
- client
- web application

Total Applications Supported in Vulnerability Database Update 340

Cisco Vulnerability Database (VDB) Update 340 supports 3,571 applications.

Vulnerability Database Update 340 Changelog

This section describes the changes from VDB 339 (9:41:10 PM on November 5th, 2020 UTC) to VDB 340 (12:15:58 AM on December 16th, 2020 UTC).

Application Protocol Detectors

Total Added:	0
Total Removed:	0
Total Updated	5

Client Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Web Application Detectors

Total Added:	2
Total Removed:	23
Total Updated	15

FireSIGHT/Firepower Detector Updates

Total Added:	0
Total Removed:	0
Total Updated	0

Operating System Fingerprint Details

Total Added:	0
Total Removed:	0
Total Updated	0

Operating System and Hardware Fingerprint Details

Total Added:	0
Total Removed:	0
Total Updated	0

Vulnerability References

Total Added:	54
Total Removed:	0
Total Updated	0

Fingerprint References

Total Added:	0
Total Removed:	0
Total Updated	0

File Type Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Operating System Fingerprint Details:

- no additions or modifications

Operating System and Hardware Fingerprint Details:

- no additions or modifications

Fingerprint Reference Details:

- no additions or modifications

Application Protocol Detectors:

- QUIC: Added coverage for Quic version 50 (Updated)
- SNMP: Added coverage to detect SNMP flows (Updated)
- SSL: Fixed false positives for some HTTP2 flows that were getting classified as SSL (Updated)
- DNS: Updated detector to detect flows properly (Updated)
- UDP: Updated detector for further metadata extractions (Updated)

Client Detectors:

- no additions or modifications

Web Application Detectors:

- Plaxo: An online address book and social networking service that provides automatic updating of contact information. (Removed)
- AOL Instant Messenger: AOL's internet chat client. (Removed)
- AOL Instant Messenger Netscape: AOL Instant Messenger - Netscape. (Removed)

- Scottrade: Discount brokerage service. (Removed)
- Vehix: New and used car information and sales website. (Removed)
- GOGOBOX: Chinese based web portal. (Removed)
- Suresome: Web based encrypted proxy service. (Removed)
- Steam: Added patterns for coverage (Updated)
- Pool Live: Facebook billiards game. (Removed)
- Datei.to: German file sharing service. (Removed)
- Apple Mobile Yahoo API: Yahoos Mobile Applications for Apple product. (Removed)
- Magicland: Facebook game application. (Removed)
- Jdistatic: Cloud-based backup service. (Removed)
- BackWeb: Software that enables automatic background software downloads and installations. (Removed)
- JetSetMe: A mobile application that allows tracking of the user's movements around the globe. (Removed)
- Chinaren: Chinese social networking site. (Removed)
- UltraViolet: Cloud-based movie streaming service. (Removed)
- Instagram Images: Traffic generated while viewing images in Instagram Media, deprecated in favor of Instagram. (Removed)
- Instagram Video: Traffic generated while viewing videos in Instagram Media, deprecated in favor of Instagram. (Removed)
- Songsari: Korean webportal for Online and download media files. (Removed)
- Yandex Music: Added patterns for coverage (Updated)
- Yandex Video: Added patterns for coverage (Updated)
- Best Arabic Games: Arabic-language online casino. (Removed)
- PandaTv: Live-streaming video platform for gamers. (Removed)
- YNews: General ybreakingnews.com website traffic. (Removed)
- Adult World: Adult Videos. (Removed)
- Instagram Media: Traffic generated while viewing images and videos in Instagram. (Added)
- TikTok: Added a new detector which will cover previous Musical.ly coverage. (Added)
- Staples: Added coverage (Updated)
- Google Translate: Added geographical patterns for the website (Updated)
- GoDaddy: Added patterns for coverage (Updated)
- BlueStacks: Added patterns for coverage (Updated)
- Angry Birds: Added patterns for coverage (Updated)
- Turbo VPN: Added patterns for coverage (Updated)

- Zynga Poker: Added patterns for coverage (Updated)
- DotVPN: Added patterns for coverage (Updated)
- Gom VPN: Added patterns for coverage (Updated)
- Express VPN: Added patterns for coverage (Updated)
- Sony: Added geographical patterns for the website (Updated)
- Facebook Video: Added coverage (Updated)

FireSIGHT/Firepower Detector Updates:

- no additions or modifications

File Type Detector Details:

- no additions or modifications

Snort ID Vulnerability Reference Details:

- CVE: 2017-11284 - Snort Reference ID 56407,56406,46937 (Added)
- CVE: 2018-18264 - Snort Reference ID 56439 (Added)
- CVE: 2019-11580 - Snort Reference ID 56436 (Added)
- CVE: 2019-12630 - Snort Reference ID 56407,56406,46937 (Added)
- CVE: 2019-1621 - Snort Reference ID 50514,56306 (Added)
- CVE: 2019-18257 - Snort Reference ID 56386,56385,56384,56383 (Added)
- CVE: 2019-2904 - Snort Reference ID 56499,56498,56497 (Added)
- CVE: 2019-7192 - Snort Reference ID 56521,56520 (Added)
- CVE: 2020-10243 - Snort Reference ID 56525,56524,56523 (Added)
- CVE: 2020-14625 - Snort Reference ID 56445,37859 (Added)
- CVE: 2020-1472 - Snort Reference ID 56290,55802,55704,55703 (Added)
- CVE: 2020-14882 - Snort Reference ID 56203,56202,56201,56200 (Added)
- CVE: 2020-15299 - Snort Reference ID 56325,56324 (Added)
- CVE: 2020-15999 - Snort Reference ID 56133,56132,56131,56130 (Added)
- CVE: 2020-16998 - Snort Reference ID 56255,56254 (Added)
- CVE: 2020-17010 - Snort Reference ID 56264,56263 (Added)
- CVE: 2020-17038 - Snort Reference ID 56262,56261 (Added)
- CVE: 2020-17047 - Snort Reference ID 56309 (Added)
- CVE: 2020-17051 - Snort Reference ID 56312,56311 (Added)
- CVE: 2020-17052 - Snort Reference ID 56287,56286 (Added)

- CVE: 2020-17053 - Snort Reference ID 56289,56288 (Added)
- CVE: 2020-17056 - Snort Reference ID 56302,56301 (Added)
- CVE: 2020-17057 - Snort Reference ID 56260,56259 (Added)
- CVE: 2020-17061 - Snort Reference ID 56305,56304,56303 (Added)
- CVE: 2020-17087 - Snort Reference ID 56231,56230 (Added)
- CVE: 2020-17088 - Snort Reference ID 56296,56295 (Added)
- CVE: 2020-1747 - Snort Reference ID 56224,56223 (Added)
- CVE: 2020-24948 - Snort Reference ID 56519 (Added)
- CVE: 2020-26072 - Snort Reference ID 56448 (Added)
- CVE: 2020-26567 - Snort Reference ID 56364 (Added)
- CVE: 2020-27125 - Snort Reference ID 56408 (Added)
- CVE: 2020-27130 - Snort Reference ID 56423,56422,56421,56420,56419,56418,56417,56416,56415,56414,56405,56404 (Added)
- CVE: 2020-27131 - Snort Reference ID 56413,56412,56411,56410,56409,56408,56407,56406,46937 (Added)
- CVE: 2020-3367 - Snort Reference ID 49992,49993,49994,49995 (Added)
- CVE: 2020-3371 - Snort Reference ID 47698 (Added)
- CVE: 2020-3392 - Snort Reference ID 56447 (Added)
- CVE: 2020-3470 - Snort Reference ID 56440,56441,56442,56443,56444 (Added)
- CVE: 2020-3531 - Snort Reference ID 56431 (Added)
- CVE: 2020-3556 - Snort Reference ID 56221,56222 (Added)
- CVE: 2020-3573 - Snort Reference ID 56216,56217 (Added)
- CVE: 2020-3586 - Snort Reference ID 56424 (Added)
- CVE: 2020-3588 - Snort Reference ID 56225 (Added)
- CVE: 2020-3603 - Snort Reference ID 56216,56217 (Added)
- CVE: 2020-3604 - Snort Reference ID 56218,56219 (Added)
- CVE: 2020-4206 - Snort Reference ID 56430,56429,56428,56427 (Added)
- CVE: 2020-4208 - Snort Reference ID 56321 (Added)
- CVE: 2020-4241 - Snort Reference ID 56435,56434,56433,56432 (Added)
- CVE: 2020-6147 - Snort Reference ID 54308,54309 (Added)
- CVE: 2020-6148 - Snort Reference ID 54310,54311 (Added)
- CVE: 2020-6149 - Snort Reference ID 54312,54313 (Added)
- CVE: 2020-6150 - Snort Reference ID 54314,54315 (Added)

- CVE: 2020-6155 - Snort Reference ID 54415,54416 (Added)
- CVE: 2020-6156 - Snort Reference ID 54430,54431 (Added)
- CVE: 2020-6549 - Snort Reference ID 56438,56437 (Added)

For Assistance

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco Firepower devices, see What's New in Cisco Product Documentation.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service. If you have any questions or require assistance with Cisco ASA devices, please contact Cisco Support:

- Note: To open a TAC request, you must first register for a Cisco.com user ID
- Once you have a Cisco.com user ID, you may initiate or check on the status of a service request online or contacting the TAC by phone:
  - U.S. - 1-800-553-2447 Toll Free
  - International support numbers
- For additional information on obtaining technical support through the TAC, please consult the Technical Support Reference Guide (PDF - 1 MB)

About Talos

The Talos Security Intelligence and Research Group (Talos) is made up of leading threat researchers supported by sophisticated systems to create threat intelligence for Cisco products that detects, analyzes and protects against both known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, SenderBase.org and SpamCop. The team's expertise spans software development, reverse engineering, vulnerability triage, malware investigation and intelligence gathering.