Release Notes for Cisco Vulnerability Database (VDB) Update 297

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.

The Cisco Talos Security Intelligence and Research Group (Talos) 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 297

Cisco Vulnerability Database (VDB) Update 297 supports 3,626 applications.

Vulnerability Database Update 297 Changelog

This section describes the changes from VDB 294 (12:36:33 AM on February 9th, 2018 UTC) to VDB 297 (7:53:06 PM on March 16th, 2018 UTC).

Application Protocol Detectors

Total Added:	1
Total Removed:	1
Total Updated	0

Client Detectors

Total Added:	3
Total Removed:	0
Total Updated	0

Web Application Detectors

Total Added:	8
Total Removed:	2
Total Updated	0

FireSIGHT/Firepower Detector Updates

Total Added:	10
Total Removed:	1
Total Updated	0

Operating System Fingerprint Details

Total Added:	3
Total Removed:	0
Total Updated	13

Operating System and Hardware Fingerprint Details

Total Added:	21
Total Removed:	0
Total Updated	0

Vulnerability References

Total Added:	0
Total Removed:	0
Total Updated	0

Fingerprint References

Total Added:	17
Total Removed:	1
Total Updated	3

File Type Detectors

Total Added:	0
Total Removed:	0
Total Updated	1

Operating System Fingerprint Details:

- Apple Mac OSX 10.13.1 (ID 130070) (added)
- Apple Mac OSX 10.13.2 (ID 130071) (added)
- Apple Mac OSX 10.13.3 (ID 130072) (added)
- Apple Mac OSX; iOS Mac_OSX 10.5, 10.6, 10.7, 10.8, 10.9 ; iOS 5.1, 6.0, 6.1 (ID 924) (updated)
- Apple Mac OSX 10.5, 10.6, 10.10, 10.11, 10.12, 10.13 (ID 925) (updated)
- Microsoft Windows, Windows Phone 98, Server 2008, Server 2008 R2, 7, 8; 7.5 (ID 30003) (updated)
- Linux or Google Linux kernel or Android Linux kernel 2.6 or Android 2.2, 2.3 (ID 30901) (updated)
- Apple Mac OSX 10.4 - 10.5 (ID 30920) (updated)
- Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.7; iOS 3.1, 4.2 (ID 30922) (updated)
- Apple Mac OSX or iOS Mac_OSX 10.5, 10.6, 10.7, 10.8, 10.9 or iOS 5.0, 5.1, 6.0, 6.1, 7.0, 7.1, 8.1, 8.4, 9.1 (updated)
- Apple Mac OSX or iOS Mac_OSX 10.5,10.6,10.10,10.11,10.12,10.13 or iOS 8.0,8.1,8.2,8.3,8.4,9.0,9.1,9.2 ... (updated)
- Apple Mac OSX or iOS Mac_OSX 10.5, 10.6 or Apple iOS version 11.0, 11.1, 11.2 (ID 30926) (updated)
- Cisco IronPort AsyncOS 7.6 (ID 30963) (updated)
- Apple iOS 9.0, 9.1, 9.2, 9.3, 10.0, 10.2, 11.0, 11.1, 11.2 (ID 60203) (updated)
- Apple Mac OSX 10.11, 10.12, 10.13 (ID 60204) (updated)
- Microsoft Windows 7, Server 2008 R2 (ID 130021) (updated)

Operating System and Hardware Fingerprint Details:

- Apple iOS 11.1 (ID 70229) (added)
- Apple iOS 11.1 (ID 70230) (added)
- Apple iOS 11.1.1 (ID 70231) (added)
- Apple iOS 11.1.1 (ID 70232) (added)
- Apple iOS 11.1.2 (ID 70233) (added)
- Apple iOS 11.1.2 (ID 70234) (added)
- Apple iOS 11.2 (ID 70235) (added)
- Apple iOS 11.2 (ID 70236) (added)
- Apple iOS 11.2.1 (ID 70237) (added)
- Apple iOS 11.2.1 (ID 70238) (added)
- Apple iOS 11.2.2 (ID 70239) (added)
- Apple iOS 11.2.2 (ID 70240) (added)
- Apple iOS 11.2.5 (ID 70241) (added)
- Apple iOS 11.2.5 (ID 70242) (added)
- Apple iOS iPhone 8 Plus (ID 100232) (added)
- Apple iOS iPhone 8 Plus (ID 100233) (added)
- Apple iOS iPhone 8 Plus (ID 100234) (added)
- Google Android Samsung Galaxy S8 (ID 100235) (added)
- Apple iOS iPad Pro 1st Gen (ID 100236) (added)
- Apple iOS iPad Pro 1st Gen (ID 100237) (added)
- Apple iOS iPad Pro 1st Gen (ID 100238) (added)

Fingerprint Reference Details:

- Fingerprint ID 309585 references (removed)
- Fingerprint ID 70229 references (added)
- Fingerprint ID 70230 references (added)
- Fingerprint ID 70231 references (added)
- Fingerprint ID 70232 references (added)
- Fingerprint ID 70233 references (added)
- Fingerprint ID 70234 references (added)
- Fingerprint ID 70235 references (added)
- Fingerprint ID 70236 references (added)
- Fingerprint ID 70237 references (added)

- Fingerprint ID 70238 references (added)
- Fingerprint ID 70239 references (added)
- Fingerprint ID 70240 references (added)
- Fingerprint ID 70241 references (added)
- Fingerprint ID 70242 references (added)
- Fingerprint ID 130070 references (added)
- Fingerprint ID 130071 references (added)
- Fingerprint ID 130072 references (added)
- Fingerprint ID 925 references (updated)
- Fingerprint ID 30926 references (updated)
- Fingerprint ID 60203 references (updated)

Application Protocol Detectors:

- VMware Remote Authentication: VMware Daemon for authentication of remote VMs. (added)
- VNC: Graphical desktop sharing protocol.

Client Detectors:

- Psiphon: Web proxy/anonymizer. (added)
- QUIC: Quick UDP Internet Connections, an experimental, mutliplexing transport layer protocol. (added)
- Ultrasurf: Freeware anti-censorship proxy. (added)

Web Application Detectors:

- 21 Questions: Social quiz game. (removed)
- eNovance: Advertisement site. (removed)
- Apple Maps: Apple maps and navigation. (added)
- MKRU: News website for the Russian newspaper Moskovskij Komsomolets. (added)
- MKRU Streaming: Live streaming for the Russian newspaper Moskovskij Komsomolets. (added)
- Office 365: Traffic generated by MS Office 365 applications and web services. (added)
- Plex TV: Allows users to stream their own media from one device to others over the Plex TV network. (added)
- Zoho Chat: A web-enabled group chat application. (added)
- Zoho Mail: Zoho webmail. (added)
- Zoho Wiki: Zoho collaborative web space. (added)

FireSIGHT/Firepower Detector Updates:

- uTorrent: BitTorrent client known for its lightweight and efficient design. (added)

- Sophos Live Protection: Anti-Malware software. (added)
- Hoxx VPN: An anonymizer and tunnelling software that encrypts web traffic. (added)
- Sports Illustrated: Web portal for sports news and updates. (added)
- Data Saver: A chrome extension offered by Google for saving data usage. (added)
- iflix: Movie streaming. (added)
- HideMyIp VPN: VPN traffic generated by HideMyIp vpn. (added)
- Hide.me VPN: VPN traffic generated by Hide.me vpn. (added)
- ITU H.245 Audio: An ITU-specified control channel protocol used with H.323 and H.324 audio sessions. (added)
- U.S State: U.S. Department of State website. (added)
- VNC: Graphical desktop sharing protocol. (removed)

File Type Detector Details:

- MKV Matroska stream file (ID 238) (updated)

Snort ID Vulnerability Reference Details:

- no additions or modifications

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.