Release Notes for Cisco Vulnerability Database (VDB) Update 303

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 303

Cisco Vulnerability Database (VDB) Update 303 supports 3,618 applications.

Vulnerability Database Update 303 Changelog

This section describes the changes from VDB 300 (3:32:02 PM on July 3rd, 2018 UTC) to VDB 303 (2:30:24 PM on August 3rd, 2018 UTC).

Application Protocol Detectors

Total Added:	0
Total Removed:	1
Total Updated	0

Client Detectors

Total Added:	0
Total Removed:	1
Total Updated	0

Web Application Detectors

Total Added:	1
Total Removed:	10
Total Updated	10

FireSIGHT/Firepower Detector Updates

Total Added:	0
Total Removed:	5
Total Updated	0

Operating System Fingerprint Details

Total Added:	0
Total Removed:	0
Total Updated	2

Operating System and Hardware Fingerprint Details

Total Added:	7
Total Removed:	0
Total Updated	0

Vulnerability References

Total Added:	0
Total Removed:	0
Total Updated	0

Fingerprint References

Total Added:	6
Total Removed:	0
Total Updated	2

File Type Detectors

Total Added:	0
Total Removed:	0
Total Updated	1

Operating System Fingerprint Details:

- Apple Mac OSX or iOS Mac OSX 10.5, 10.6 or Apple iOS version 11.0, 11.1, 11.2, 11.3, 11.4 (ID 30926) (updated)

- Apple iOS 9.0, 9.1, 9.2, 9.3, 10.0, 10.2, 11.0, 11.1, 11.2, 11.3, 11.4 (ID 60203) (updated)

Operating System and Hardware Fingerprint Details:

- Apple iOS 11.3.1 (ID 70250) (added)

- Apple iOS 11.3.1 (ID 70251) (added)

- Apple iOS 11.3.1 (ID 70252) (added)

- Apple iOS 11.4 (ID 70253) (added)

- Apple iOS 11.4 (ID 70254) (added)

- Apple iOS 11.4 (ID 70255) (added)

- Apple iOS iPhone 8 Plus (ID 100239) (added)

Fingerprint Reference Details:

- Fingerprint ID 70250 references (added)

- Fingerprint ID 70251 references (added)

- Fingerprint ID 70252 references (added)

- Fingerprint ID 70253 references (added)

- Fingerprint ID 70254 references (added)

- Fingerprint ID 70255 references (added)

- Fingerprint ID 30926 references (updated)

- Fingerprint ID 60203 references (updated)

Application Protocol Detectors:

- FireAMP: Obsolete in all product versions (removed)

Client Detectors:

- FireAMP: Obsolete in all product versions (removed)

Web Application Detectors:

- Channel Intelligence: Advertising platform. (removed)

- Cisco Jabber Video: Video conferencing with Cisco's instant messenger. (removed)

- Empower Network: Online Marketing strategy and traffic analyzer. (removed)

- FireAMP: Cloud-based real time antivirus protection. (added)

- FireAMP SSL: Connection to FireAMP cloud. (removed)

- Glam: News regarding recent trends in fashion and lifestyle. (removed)

- Grooveshark: Online music search engine and streaming service. (removed)

- Kanoodle: Web advertisement services. (removed)

- Megashares: File hosting and sharing service. Distinct from Megashare. (removed)

- Olive Media: Advertisement site. (removed)

- Pulse360: Web advertisement services. (removed)

- Sap: Improvements on the SAP NetWeaver traffic (updated)

- Slack: Improvements on slack traffic where it was previously recognized as WhatsApp (updated)

- Turbovpn: Improvements on the detection for TurboVPN (updated)

- Softether: Improvements on the detection of the SoftEther VPN (updated)

- QQ: Improvements on the detection of QQ traffic (updated)

- WeChat: Improvements on the WeChat traffic (updated)

- WhatsApp: Improvements on the WhatsApp to identify WhatsApp Chats (updated)

- YouTube: Improvements on the detection of YouTube streaming (updated)

- QUIC: Improvements on QUIC detection (updated)

- Google: Improvements of the detection from Google (updated)

FireSIGHT/Firepower Detector Updates:

- Olive Media: Advertisement site. (removed)

- Grooveshark: Online music search engine and streaming service. (removed)

- Cisco Jabber Audio: Audio conferencing with Cisco's instant messenger. (removed)

- Cisco Jabber Video: Video conferencing with Cisco's instant messenger. (removed)

- Megashares: File hosting and sharing service. Distinct from Megashare. (removed)

File Type Detector Details:

- VB Microsoft Visual Basic files, including .cs, .vb, and .vbp (ID 278) (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.