Release Notes for Cisco Vulnerability Database (VDB) Update 298

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 298

Cisco Vulnerability Database (VDB) Update 298 supports 3,621 applications.

Vulnerability Database Update 298 Changelog

This section describes the changes from VDB 297 (7:59:29 PM on March 16th, 2018 UTC) to VDB 298 (6:18:22 PM on May 15th, 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:	2
Total Removed:	9
Total Updated	0

FireSIGHT Detector Updates

Total Added:	8
Total Removed:	11
Total Updated	18

Operating System Fingerprint Details

Total Added:	1
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:	7
Total Removed:	0
Total Updated	5

File Type Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Operating System Fingerprint Details:

- Apple Mac OSX 10.13.4 (ID 130073) (added)
- Apple Mac OSX or iOS Mac_OSX 10.5, 10.6 or Apple iOS version 11.0, 11.1, 11.2, 11.3 (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 (ID 60203) (updated)

Operating System and Hardware Fingerprint Details:

- Apple iOS 10.1.1 (ID 70243) (added)
- Apple iOS 10.1.1 (ID 70244) (added)
- Apple iOS 10.1.1 (ID 70245) (added)
- Apple iOS 11.3 (ID 70246) (added)
- Apple iOS 11.3 (ID 70247) (added)
- Apple iOS 10.0.1 (ID 70248) (added)
- Apple iOS 10.0.1 (ID 70249) (added)

Fingerprint Reference Details:

- Fingerprint ID 70243 references (added)
- Fingerprint ID 70244 references (added)
- Fingerprint ID 70245 references (added)
- Fingerprint ID 70246 references (added)
- Fingerprint ID 70247 references (added)

- Fingerprint ID 70249 references (added)
- Fingerprint ID 130073 references (added)
- Fingerprint ID 925 references (updated)
- Fingerprint ID 30925 references (updated)
- Fingerprint ID 30926 references (updated)
- Fingerprint ID 60203 references (updated)
- Fingerprint ID 60204 references (updated)

Application Protocol Detectors:

- no additions or modifications

Client Detectors:

- no additions or modifications

Web Application Detectors:

- Achetez Facile: French online shopping site. (removed)
- Admasters: Advertisement site. (removed)
- Adometry: Advertisement site. (removed)
- Chrome webstore: App and extension marketplace for Chrome and Chromebook. (added)
- Google Helpouts: A social networking and instant messaging system for expert advice on various topics. (removed)
- jJcast: Video management and streaming platform. (removed)
- Meerkat: Mobile app for live video streaming. (removed)
- WebEx: Obsolete in all product versions (removed)
- Office365 Admin portal: Admin portal to manage Office 365 products. (added)
- ooVoo: Video chat and instant messaging. (removed)
- Reduxmedia: Advertisement site. (removed)

FireSIGHT/Firepower Detector Updates:

- Oman Airways: Oman Airways official website. (added)
- Azure cloud portal: Microsoft Azure cloud service portal. (added)
- Watan: An Arabic newspaper. (added)
- Mathrubhumi: Malayalam newspaper published from Kerala, India. (added)
- CimaClub: Movie and video streaming website. (added)
- MawDoo3: Arabic online encyclopedia. (added)
- Windows Azure: Cloud computing by Microsoft. (added)

- Opera VPN: Free VPN integrated with the Opera browser. (added)
- Admasters: Advertisement site. (removed)
- Google Helpouts: A social networking and instant messaging system for expert advice on various topics. (removed)
- Achetez Facile: French online shopping site. (removed)
- Meerkat: Mobile app for live video streaming. (removed)
- Reduxmedia: Advertisement site. (removed)
- Nabber: General finance-lp.com website traffic. (removed)
- WhatsApp Location: WhatsApp locator services. (removed)
- Google Talk File Exchange: File exchange over google chat. (removed)
- ooVoo: Video chat and instant messaging. (removed)
- Adometry: Advertisement site. (removed)
- Ozock: Platform to create, share and discover the Worlds most viral, funny and newsworthy stories. (removed)
- Quic: Added support of QUIC version Q041. (updated)
- HideMyIP VPN: Improvements on the Hide My IP VPN (updated)
- WebEx: Improvements on the WebEx detector where some flows were identified as STUN. (updated)
- QQ: Improvements on the QQ detector. (updated)
- H323: Improvements on the H323 audio protocol. (updated)
- Google: Improvements on googles traffic where it was sometimes getting identified as QUIC, and Google Videos (updated)
- Hotspot Shield: Improvements on Hotspot Shield where some traffic flows were getting misidentified as Facebook. (updated)
- GoToMeeting: Improvements on the detection of the GoToMeeting Protocol. (updated)
- Google Hangouts: Improvements on Google Hangouts where some flows were previously classified as WebRTC (updated)
- KakaoTalk: Improvements on Kakao Talk's traffic (updated)
- LogMeIn: Improvements on the LogMeIn's SSL traffic (updated)
- Telegram: Improvements on the Telegram detector (updated)
- Netflix: Improvements the detection of the Netflix detector (updated)
- Uber: Improvements of the Uber detector (updated)
- Skype: Updated the Skype detector where some Skype traffic flows were recognized as Stun. (updated)
- Snapchat: Updated the Snapchat plug-in, as some Snapchat traffic flows were recognized as SSL, Quic, and Google. (updated)

- YouTube: Improvements on YouTube traffic. (updated)

File Type Detector Details:

- no additions or modifications

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.