Release Notes for Cisco Vulnerability Database (VDB) Update 304

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 304

Cisco Vulnerability Database (VDB) Update 304 supports 3,608 applications.

Vulnerability Database Update 304 Changelog

This section describes the changes from VDB 303 (2:30:24 PM on August 3rd, 2018 UTC) to VDB 304 (4:53:32 PM on September 6th, 2018 UTC).

Application Protocol Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Client Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Web Application Detectors

Total Added:	0
Total Removed:	8
Total Updated	9

FireSIGHT/Firepower Detector Updates

Total Added:	1
Total Removed:	9
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:	0
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:

- no additions or modifications

Client Detectors:

- no additions or modifications

Web Application Detectors:

- 100ye.com: Chinese search portal. (removed)
- Docstoc: Electronic business document repository and online store. (removed)
- Docstoc Upload: Electronic repository for documents, video. (removed)
- Livemeeting: Microsoft's commercial web-conferencing service. (removed)
- LiveRail: Advertisement site. (removed)
- Mafiawars: A multiplayer browser game created by Zynga. It is on several social networking sites and on the iPhone. (removed)
- Tritone Hosting: Advertisement and analytics site. (removed)

- Washington Post Social Reader: App that allows Facebook and the Washington Post to map users to the news links they click on. (removed)
- WEBRTC: Improvements over the detection of WebRTC traffic flows (updated)
- IMO: Improvements over the detection of IMO traffic (updated)
- XVPN: Improvements over the detection of XVPN application (updated)
- Doubleclick: Fixed issues where some Doubleclick flows were previously classified as GoogleDocs (updated)
- GoToMeeting: Improvements on the audio/video detection for GotoMeeting traffic (updated)
- Psiphon: Improvements over the SSH flows under Psiphon (updated)
- SoftEther: Improvements over the SoftEther traffic flows (updated)
- Ares: Improvements over the Ares traffic flows (updated)
- Facebook: Improvements over the Facebook detection (updated)

FireSIGHT/Firepower Detector Updates:

- PureVPN: Traffic generated by PureVPN. (added)
- Mafiawars: A multiplayer browser game created by Zynga. It is on several social networking sites and on the iPhone. (removed)
- Docstoc: Electronic business document repository and online store. (removed)
- QQ Shopping: Tencent shopping sites. (removed)
- Livemeeting: Microsoft's commercial web-conferencing service. (removed)
- Storehouse: Traffic generated by Storehouse, tool to create stories using photos and videos. (removed)
- Citrix GoToMeeting Platform: GotoMeeting platform based services. (removed)
- DNP3: Process automation protocol, commonly used to control equipment used by utilities such as electricity and water. (removed)
- Tritone Hosting: Advertisement and analytics site. (removed)
- LiveRail: Advertisement site. (removed)

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.