Release Notes for Cisco Vulnerability Database (VDB) Update 337

- About the Cisco Vulnerability Database, on page 2
- About the Cisco Firepower Application Detector Reference, on page 3
- Supported Platforms and Software Versions, on page 4
- Supported Detector Types, on page 5
- Total Applications Supported in Vulnerability Database Update 337, on page 6
- Vulnerability Database Update 337 Changelog, on page 7
- For Assistance, on page 11
- About Talos, on page 12

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 337

Cisco Vulnerability Database (VDB) Update 337 supports 3,665 applications.

Vulnerability Database Update 337 Changelog

This section describes the changes from VDB 336 (4:39:44 PM on June 15th, 2020 UTC) to VDB 337 (4:52:14 PM on July 10th, 2020 UTC).

Application Protocol Detectors

Total Added:	0
Total Removed:	0
Total Updated	5

Client Detectors

Total Added:	0
Total Removed:	0
Total Updated	2

Web Application Detectors

Total Added:	15
Total Removed:	0
Total Updated	10

FireSIGHT/Firepower Detector Updates

Total Added:	0
Total Removed:	0
Total Updated	7

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:

In this release, we have introduced a more streamlined method for syncing our latest Vulnerability data from the National Vulnerability Database (NVD). This change allows us to have more up-to-date vulnerability references that are directly synchronized with our current IPS rules and the published NVD data.

- Last Updated: July 2, 2020
- Total Vulnerabilities: 11,146
- Updated 83,000 software entries and deprecated the old software entries.

These optimizations have also helped to reduce the overall VDB package size down to the 10MB range.

Application Protocol Detectors:

- Battle.net: Modified detector to avoid false positives (Updated)
- SSL: Modified detector to extract new metadata. (Updated)
- DNS: Modified detector to extract new metadata. (Updated)
- IMAP: Modified detector to improve detection (Updated)
- HTTP: Modified detector to distinguish tunneled flows (Updated)

Client Detectors:

- Psiphon: Modified detector to improve detection of flows over proxy (Updated)
- Ultrasurf: Modified detector to improve detection of flows over proxy (Updated)

Web Application Detectors:

- Bing Maps: Modified detector for better coverage (Updated)
- MTv: Modified detector for better coverage (Updated)
- VPN Master: Modified detector for better coverage (Updated)
- Adobe Update: Updates for Adobe software. (Added)
- DriveHQ: Cloud storage and online backup system. (Added)
- IEC 104 Control Bitstring 32 bits: IoT based detector (Added)
- IEC 104 Double Command: IoT based detector (Added)
- IEC 104 Interrogation Command: IoT based detector (Added)
- IEC 104 Regulating Step Command: IoT based detector (Added)
- IEC 104 Setpoint Command Normalized: IoT based detector (Added)
- IEC 104 Setpoint Command Scaled: IoT based detector (Added)
- IEC 104 Setpoint Command Short Float: IoT based detector (Added)
- IEC 104 End of Initialization: IoT based detector (Added)
- IEC 104 Measured Normalized with Long Time: IoT based detector (Added)
- IEC 104 Single Point Info with Long Time: IoT based detector (Added)
- IEC 104 Step Position Info: IoT based detector (Added)
- IEC 104 Measured Short Float: IoT based detector (Added)
- IEC 104 Single Point Info: IoT based detector (Added)
- Twitter: Modified detector for better coverage (Updated)
- Box: Modified detector for better coverage (Updated)
- Blizzard: Modified detector for better coverage (Updated)
- Wii: Modified detector for better coverage (Updated)
- DuckDuckGo: Modified detector to provide better coverage for safesearch (Updated)
- eRoom: Modified detector to remove false positive for Nintendo gaming traffic (Updated)
- Zoom: Modified detector to add coverage for certain UDP traffic (Updated)

FireSIGHT/Firepower Detector Updates:

- QQ: Modified detector to improve detection and memory usage. (Updated)
- OpenVPN: Modified detector to improve detection and memory usage. (Updated)

- RTP: Modified detector to improve detection and memory usage. (Updated)
- Fuze: Modified detector to avoid false positives on RTP traffic (Updated)
- Exchange: Modified detector for better coverage (Updated)
- Salesforce.com: Modified detector for better coverage (Updated)
- Microsoft: Modified detector for better coverage (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.