Release Notes for Cisco Vulnerability Database (VDB) Update 343

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 343

Cisco Vulnerability Database (VDB) Update 343 supports 3,697 applications.

Vulnerability Database Update 343 Changelog

This section describes the changes from VDB 342 (8:56:05 PM on March 29th, 2021 UTC) to VDB 343 (1:08:38 AM on May 21st, 2021 UTC).

Application Protocol Detectors

Total Added:	80
Total Removed:	0
Total Updated	2

Client Detectors

Total Added:	2
Total Removed:	0
Total Updated	0

Web Application Detectors

Total Added:	0
Total Removed:	13
Total Updated	9

FireSIGHT/Firepower Detector Updates

Total Added:	0
Total Removed:	0
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:	84
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:

- QUIC: Added coverage for UDP flows. (Updated)
- Radius: Added coverage for UDP flows. (Updated)
- MMS unconfirmedPDU: An MMS Unconfirmed PDU message. (Added)
- MMS confirmedResponsePDU: An MMS Confirmed Response PDU message. (Added)
- MMS read: An MMS Command of Read request. (Added)
- MMS write: An MMS Command of Write request. (Added)
- MMS getVariableAccAttr: An MMS Command of Get Variable Access Attributes request. (Added)
- MMS getNamedVariableListAttr: An MMS Command of Get Named Variable List Attributes request. (Added)
- MMS confirmedErrorPDU: An MMS Confirmed Error PDU message. (Added)
- MMS status: An MMS Command of Status request. (Added)
- MMS identify: An MMS Command of Identify request. (Added)

- MMS rename: An MMS Command of Rename request. (Added)
- MMS defineNamedVariable: An MMS Command of Define Named Variable request. (Added)
- MMS defineScatteredAccess: An MMS Command of Define Scattered Access request. (Added)
- MMS getScatteredAccessAttr: An MMS Command of Get Scattered Access Attributes request. (Added)
- MMS deleteVariableAccess: An MMS Command of Delete Variable Access request. (Added)
- MMS defineNamedVariableList: An MMS Command of Define Named Variable List request. (Added)
- MMS deleteNamedVariableList: An MMS Command of Delete Named Variable List request. (Added)
- MMS defineNamedType: An MMS Command of Define Named Type request. (Added)
- MMS getNamedTypeAttr: An MMS Command of Get Named Type Attributes request. (Added)
- MMS deleteNamedType: An MMS Command of Delete Named Type request. (Added)
- MMS input: An MMS Command of Input request. (Added)
- MMS output: An MMS Command of Output request. (Added)
- MMS takeControl: An MMS Command of Take Control request. (Added)
- MMS relinquishControl: An MMS Command of Relinquish Control request. (Added)
- MMS defineSemaphore: An MMS Command of Define Semaphore request. (Added)
- MMS deleteSemaphore: An MMS Command of Delete Semaphore request. (Added)
- MMS reportSemaphoreStatus: An MMS Command of Report Semaphore Status request. (Added)
- MMS reportPoolSemaphoreStatus: An MMS Command of Report Pool Semaphore Status request. (Added)
- MMS reportSemaphoreEntryStatus: An MMS Command of Report Semaphore Entry Status request. (Added)
- MMS initiateDownloadSequence: An MMS Command of Initiate Download Sequence request. (Added)
- MMS downloadSegment: An MMS Command of Download Segment request. (Added)
- MMS terminateDownloadSequence: An MMS Command of Terminate Download Sequence request. (Added)
- MMS initiateUploadSequence: An MMS Command of Initiate Upload Sequence request. (Added)
- MMS uploadSegment: An MMS Command of Upload Segment request. (Added)
- MMS terminateUploadSequence: An MMS Command of Terminate Upload Sequence request. (Added)
- MMS domainDownload: An MMS Command of Request Domain Download. (Added)
- MMS domainUpload: An MMS Command of Request Domain Upload. (Added)
- MMS loadDomainContent: An MMS Command of Load Domain Content request. (Added)
- MMS storeDomainContent: An MMS Command of Store Domain Content request. (Added)
- MMS deleteDomain: An MMS Command of Delete Domain request. (Added)

- MMS getDomainAttributes: An MMS Command of Get Domain Attributes request. (Added)
- MMS createProgramInvocation: An MMS Command of Create Program Invocation request. (Added)
- MMS deleteProgramInvocation: An MMS Command of Delete Program Invocation request. (Added)
- MMS start: An MMS Command of Start request. (Added)
- MMS stop: An MMS Command of stop request. (Added)
- MMS resume: An MMS Command of Resume request. (Added)
- MMS reset: An MMS Command of Reset request. (Added)
- MMS kill: An MMS Command of Kill request. (Added)
- MMS getProgramInvocationAttr: An MMS Command of Get Program Invocation Attributes request. (Added)
- MMS obtainFile: An MMS Command of Obtain File request. (Added)
- MMS defineEventCondition: An MMS Command of Define Event Condition request. (Added)
- MMS deleteEventCondition: An MMS Command of Delete Event Condition request. (Added)
- MMS getEventConditionAttr: An MMS Command of Get Event Condition Attributes request. (Added)
- MMS reportEventConditionStatus: An MMS Command of Report Event Condition Status request. (Added)
- MMS alterEventConditionMonitoring: An MMS Command of Alter Event Condition Monitoring request. (Added)
- MMS triggerEvent: An MMS Command of Trigger Event request. (Added)
- MMS defineEventAction: An MMS Command of Define Event Action request. (Added)
- MMS deleteEventAction: An MMS Command of Delete Event Action request. (Added)
- MMS getEventActionAttr: An MMS Command of Get Event Action Attributes request. (Added)
- MMS reportEventActionStatus: An MMS Command of Report Event Action Status request. (Added)
- MMS defineEventEnrollment: An MMS Command of Define Event Enrollment request. (Added)
- MMS deleteEventEnrollment: An MMS Command of Delete Event Enrollment request. (Added)
- MMS alterEventEnrollment: An MMS Command of Alter Event Enrollment request. (Added)
- MMS reportEventEnrollmentStatus: An MMS Command of Report Event Enrollment Status request. (Added)
- MMS getEventEnrollmentAttr: An MMS Command of Get Event Enrollment Attributes request. (Added)
- MMS ackEventNotificaton: An MMS Command of Acknowledge Event Notification request. (Added)
- MMS getAlarmSummary: An MMS Command of Get Alarm Summary request. (Added)
- MMS getAlarmEnrollmentSummary: An MMS Command of Get Alarm Enrollment Summary request. (Added)
- MMS readJournal: An MMS Command of Read Journal request. (Added)

- MMS writeJournal: An MMS Command of Write Journal request. (Added)
- MMS initializeJournal: An MMS Command of Initialize Journal request. (Added)
- MMS reportJournalStatus: An MMS Command of Report Journal Status request. (Added)
- MMS createJournal: An MMS Command of Create Journal request. (Added)
- MMS deleteJournal: An MMS Command of Delete Journal request. (Added)
- MMS getCapabilityList: An MMS Command of Get Capability List request. (Added)
- MMS fileOpen: An MMS Command of File Open request. (Added)
- MMS fileRead: An MMS Command of File Read request. (Added)
- MMS fileClose: An MMS Command of File Close request. (Added)
- MMS fileRename: An MMS Command of File Rename request. (Added)
- MMS fileDelete: An MMS Command of File Delete request. (Added)
- MMS fileDirectory: An MMS Command of File Directory request. (Added)

Client Detectors:

- Signal: Signal is a cross-platform centralized encrypted messaging service developed by the Signal Technology Foundation and Signal Messenger LLC. (Added)
- MongoDB: Source-available cross-platform document-oriented database program. (Added)

Web Application Detectors:

- Farmville: A real-time farm simulation game developed by Zynga, available for Facebook and the iPhone. (Removed)
- PC Mall: Name changed to Insight. (Updated)
- Bubble Island: Social bubble bursting game for Facebook. (Removed)
- Isoball: Web game where you must construct a track to lead a ball into a hole. (Removed)
- PixelMags: Content delivery network for digital versions of magazine. (Removed)
- Blekko: Search engine based on categories. (Removed)
- BlekkoBot: Web crawler for Blekko. (Removed)
- Tribal Fusion: Data-driven advertising service. (Removed)
- ValueClick: Name changed to Epsilon and added patterns for coverage. (Updated)
- MediaMind: Name changed to Sizmek Ad Suite and added patterns for coverage. (Updated)
- Brightroll: Name changed to Verizon Media (Updated)
- RadiumOne: Name changed to RythmOne (Updated)
- Hyves: Added patterns for coverage (Updated)
- blinkx: Video search engine. (Removed)

- Camo Proxy: Online free proxy server. (Removed)
- Crashlytics: Name changed to Firebase Crashlytics and added patterns for coverage. (Updated)
- Avocarrot: Mobile ad traffic. (Removed)
- ShorTel Sky Communicator: Unified communications software. (Removed)
- OnTests.Me: General ontests.me website traffic. (Removed)
- WittyFeed: Internet media which publishes viral content including sports, news, fashion, travel and inspiration. (Removed)
- YouTubeMp3: Added patterns for coverage (Updated)
- Plex TV: Added patterns for coverage (Updated)

FireSIGHT/Firepower Detector Updates:

- no additions or modifications

File Type Detector Details:

- no additions or modifications

Snort ID Vulnerability Reference Details:

- CVE 2002-2268 - Snort Reference ID 29957,29958,300016,51962,51963,51964,51965 (Added)
- CVE 2005-3653 - Snort Reference ID 2278,25276 (Added)
- CVE 2006-0150 - Snort Reference ID 13308,57580 (Added)
- CVE 2007-0352 - Snort Reference ID 17365,300017 (Added)
- CVE 2007-0548 - Snort Reference ID 300005,43349 (Added)
- CVE 2007-1326 - Snort Reference ID 57517,57518,57519 (Added)
- CVE 2007-5561 - Snort Reference ID 15554,300018 (Added)
- CVE 2008-5354 - Snort Reference ID 17563,57533,57534 (Added)
- CVE 2009-0192 - Snort Reference ID 57536 (Added)
- CVE 2009-0993 - Snort Reference ID 15554,17669,300018 (Added)
- CVE 2012-0021 - Snort Reference ID 24697,24698,300021,34048 (Added)
- CVE 2012-5861 - Snort Reference ID 57511,57512,57513,57514,57515,57516 (Added)
- CVE 2012-5876 - Snort Reference ID 29958,300016,51962,51963,51964,51965 (Added)
- CVE 2013-1310 - Snort Reference ID 31584,31585,57484,57485 (Added)
- CVE 2013-4113 - Snort Reference ID 300012,51930 (Added)
- CVE 2013-6420 - Snort Reference ID 57575 (Added)
- CVE 2014-0113 - Snort Reference ID 300013,30944 (Added)

- CVE 2014-0502 - Snort Reference ID 29928,29929,29930,29931,32359,32360,37684,37685,57499 (Added)
- CVE 2014-3913 - Snort Reference ID 17410,300003,40880 (Added)
- CVE 2015-0273 - Snort Reference ID 34123,34124,34710,34951,57578 (Added)
- CVE 2015-0395 - Snort Reference ID 57568,57569 (Added)
- CVE 2015-4069 - Snort Reference ID 34944,57532 (Added)
- CVE 2015-5371 - Snort Reference ID 300006,300007,300008,300009,300010,300011,31771,51972,51973,51974,51975,51976 (Added)
- CVE 2015-8705 - Snort Reference ID 57579 (Added)
- CVE 2016-4553 - Snort Reference ID 300004,45569 (Added)
- CVE 2016-8723 - Snort Reference ID 300003,40880 (Added)
- CVE 2017-5444 - Snort Reference ID 300019,45476 (Added)
- CVE 2019-1867 - Snort Reference ID 50037,57576 (Added)
- CVE 2019-11941 - Snort Reference ID 57500 (Added)
- CVE 2020-3562 - Snort Reference ID 57448 (Added)
- CVE 2020-6541 - Snort Reference ID 57440,57441 (Added)
- CVE 2020-6550 - Snort Reference ID 57446,57447 (Added)
- CVE 2020-8243 - Snort Reference ID 57452,57453 (Added)
- CVE 2020-8260 - Snort Reference ID 57459 (Added)
- CVE 2020-8821 - Snort Reference ID 57432 (Added)
- CVE 2020-11854 - Snort Reference ID 57494 (Added)
- CVE 2020-13529 - Snort Reference ID 54831 (Added)
- CVE 2020-25683 - Snort Reference ID 57460 (Added)
- CVE 2020-27226 - Snort Reference ID 56486,56487,56488 (Added)
- CVE 2020-27229 - Snort Reference ID 56475,56476,56477 (Added)
- CVE 2020-27230 - Snort Reference ID 56475,56476,56477 (Added)
- CVE 2020-27231 - Snort Reference ID 56475,56476,56477 (Added)
- CVE 2020-27232 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-27237 - Snort Reference ID 56478,56479,56480 (Added)
- CVE 2020-27238 - Snort Reference ID 56478,56479,56480 (Added)
- CVE 2020-27239 - Snort Reference ID 56478,56479,56480 (Added)
- CVE 2020-27240 - Snort Reference ID 56478,56479,56480 (Added)
- CVE 2020-27241 - Snort Reference ID 56478,56479,56480 (Added)

- CVE 2020-27242 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-27243 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-27244 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-27245 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-27246 - Snort Reference ID 56481,56482,56483 (Added)
- CVE 2020-28188 - Snort Reference ID 57442,57443,57444,57445 (Added)
- CVE 2020-28593 - Snort Reference ID 56729 (Added)
- CVE 2020-28600 - Snort Reference ID 57000,57001 (Added)
- CVE 2020-35729 - Snort Reference ID 57490,57491,57492,57493 (Added)
- CVE 2021-1363 - Snort Reference ID 57523,57524,57525 (Added)
- CVE 2021-1365 - Snort Reference ID 57523,57524,57525 (Added)
- CVE 2021-1401 - Snort Reference ID 57520,57521,57522 (Added)
- CVE 2021-1421 - Snort Reference ID 50650,50651,50652,50653 (Added)
- CVE 2021-1445 - Snort Reference ID 57488 (Added)
- CVE 2021-1468 - Snort Reference ID 57537 (Added)
- CVE 2021-1493 - Snort Reference ID 57486 (Added)
- CVE 2021-1497 - Snort Reference ID 57529,57530,57531 (Added)
- CVE 2021-1498 - Snort Reference ID 57526,57527,57528 (Added)
- CVE 2021-1504 - Snort Reference ID 57489 (Added)
- CVE 2021-1505 - Snort Reference ID 57535 (Added)
- CVE 2021-1508 - Snort Reference ID 57538 (Added)
- CVE 2021-20078 - Snort Reference ID 57481,57482,57483 (Added)
- CVE 2021-21220 - Snort Reference ID 57420,57421 (Added)
- CVE 2021-21822 - Snort Reference ID 57479,57480 (Added)
- CVE 2021-21975 - Snort Reference ID 57433,57435 (Added)
- CVE 2021-21978 - Snort Reference ID 57436,57437,57438,57439 (Added)
- CVE 2021-21983 - Snort Reference ID 57434 (Added)
- CVE 2021-22893 - Snort Reference ID 57454,57455,57456,57457,57458 (Added)
- CVE 2021-22991 - Snort Reference ID 57449 (Added)
- CVE 2021-22992 - Snort Reference ID 57450 (Added)
- CVE 2021-26419 - Snort Reference ID 57542,57543 (Added)
- CVE 2021-28482 - Snort Reference ID 57487 (Added)

- CVE 2021-31166 - Snort Reference ID 300014,57549,57550 (Added)
- CVE 2021-31170 - Snort Reference ID 57539,57540 (Added)
- CVE 2021-31181 - Snort Reference ID 57548 (Added)
- CVE 2021-31188 - Snort Reference ID 57544,57545 (Added)

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.