Release Notes for Cisco Vulnerability Database (VDB) Update 341

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 341

Cisco Vulnerability Database (VDB) Update 341 supports 3,584 applications.

Vulnerability Database Update 341 Changelog

This section describes the changes from VDB 340 (12:15:58 AM on December 16th, 2020 UTC) to VDB 341 (8:02:48 PM on January 29th, 2021 UTC).

Application Protocol Detectors

Total Added:	13
Total Removed:	0
Total Updated	1

Client Detectors

Total Added:	0
Total Removed:	0
Total Updated	0

Web Application Detectors

Total Added:	0
Total Removed:	0
Total Updated	5

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:	0
Total Removed:	0
Total Updated	0

Fingerprint References

Total Added:	142
Total Removed:	0
Total Updated	0

File Type Detectors

Total Added:	0
Total Removed:	0
Total Updated	1

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:

- IEEE C37.118 Synchrophasor: IEEE C37.118 Synchrophasor Data Transfer Protocol is an IEEE standard which defines a method for exchange of synchronized phasor measurement data between power system equipment. (Added)
- IEEE C37.118 Header Frame: An IEEE C37.118 Protocol Synchrophasor Header Frame Packet. (Added)
- IEEE C37.118 Data Frame: An IEEE C37.118 Protocol Synchrophasor Data Frame Packet. (Added)
- IEEE C37.118 Configuration Frame 1: An IEEE C37.118 Protocol Synchrophasor Configuration Frame 1 Packet. (Added)
- IEEE C37.118 Configuration Frame 2: An IEEE C37.118 Protocol Synchrophasor Configuration Frame 2 Packet. (Added)
- IEEE C37.118 Configuration Frame 3: An IEEE C37.118 Protocol Synchrophasor Configuration Frame 3 Packet.(Added)
- IEEE C37.118 Command Extended Frame: An IEEE C37.118 Protocol Synchrophasor Command Extended Frame Packet. (Added)

- IEEE C37.118 Command DT On Frame: An IEEE C37.118 Protocol Synchrophasor Command Data Transmission On Frame Packet. (Added)
- IEEE C37.118 Command Send Header Frame: An IEEE C37.118 Protocol Synchrophasor Command Send Header Frame Packet. (Added)
- IEEE C37.118 Command DT Off Frame: An IEEE C37.118 Protocol Synchrophasor Command Data Transmission Off Frame Packet. (Added)
- IEEE C37.118 Command Send Configuration 1 Frame: An IEEE C37.118 Protocol Synchrophasor Command Send Configuration 1 Frame Packet. (Added)
- IEEE C37.118 Command Send Configuration 2 Frame: An IEEE C37.118 Protocol Synchrophasor Command Send Configuration 2 Frame Packet. (Added)
- IEEE C37.118 Command Send Configuration 3 Frame: An IEEE C37.118 Protocol Synchrophasor Command Send Configuration 3 Frame Packet. (Added)
- BACnet: Modified detector for additional coverage. (Updated)

Client Detectors:

- no additions or modifications

Web Application Detectors:

- TeamViewer: Modified detector for additional coverage (Updated)
- Microsoft: Modified detector for additional coverage (Updated)
- Facebook: Modified detector to avoid false positives for RTP. (Updated)
- Fuze: Modified detector to avoid false positives for RTP. (Updated)
- TikTok: Modified detector for additional coverage (Updated)

FireSIGHT/Firepower Detector Updates:

- no additions or modifications

File Type Detector Details:

- Modified file type PCAP to cover file signature of .pcapng files

Snort ID Vulnerability Reference Details:

- CVE: 2009-1536 - Snort Reference ID 15851,43807,43808,56804 (Added)
- CVE: 2011-3230 - Snort Reference ID 16642,56580 (Added)
- CVE: 2017-2910 - Snort Reference ID 44106,44107 (Added)
- CVE: 2018-6692 - Snort Reference ID 56579 (Added)
- CVE: 2019-7358 - Snort Reference ID 47721,47722 (Added)
- CVE: 2019-8394 - Snort Reference ID 56586 (Added)
- CVE: 2019-10092 - Snort Reference ID 56563 (Added)

- CVE: 2020-1176 - Snort Reference ID 56843 (Added)
- CVE: 2020-3145 - Snort Reference ID 54560,54561,54562,54563,54564,56840 (Added)
- CVE: 2020-3146 - Snort Reference ID 54560,54561,54562,54563,54564,56840 (Added)
- CVE: 2020-5791 - Snort Reference ID 56877,56878,56879,56880 (Added)
- CVE: 2020-7961 - Snort Reference ID 56799,56800,56801 (Added)
- CVE: 2020-8193 - Snort Reference ID 56138,56720 (Added)
- CVE: 2020-8257 - Snort Reference ID 56186,56187,56188 (Added)
- CVE: 2020-8258 - Snort Reference ID 56186,56187,56188 (Added)
- CVE: 2020-8271 - Snort Reference ID 56823,56824 (Added)
- CVE: 2020-10146 - Snort Reference ID 56574 (Added)
- CVE: 2020-10148 - Snort Reference ID 56825,56826,56827,56828,56829,56916,56917 (Added)
- CVE: 2020-10220 - Snort Reference ID 56545 (Added)
- CVE: 2020-10619 - Snort Reference ID 56532,56533,56534 (Added)
- CVE: 2020-10879 - Snort Reference ID 56624,56625,56626,56627 (Added)
- CVE: 2020-12388 - Snort Reference ID 56541,56542 (Added)
- CVE: 2020-13160 - Snort Reference ID 56543,56544 (Added)
- CVE: 2020-13379 - Snort Reference ID 56822 (Added)
- CVE: 2020-13493 - Snort Reference ID 54432,54433 (Added)
- CVE: 2020-13494 - Snort Reference ID 54492,54493 (Added)
- CVE: 2020-13496 - Snort Reference ID 54467,54468 (Added)
- CVE: 2020-13497 - Snort Reference ID 54469,54470 (Added)
- CVE: 2020-13498 - Snort Reference ID 54471,54472 (Added)
- CVE: 2020-13509 - Snort Reference ID 54440,54441 (Added)
- CVE: 2020-13510 - Snort Reference ID 54442,54443 (Added)
- CVE: 2020-13511 - Snort Reference ID 54444,54445 (Added)
- CVE: 2020-13512 - Snort Reference ID 54446,54447 (Added)
- CVE: 2020-13513 - Snort Reference ID 54448,54449 (Added)
- CVE: 2020-13514 - Snort Reference ID 54450,54451 (Added)
- CVE: 2020-13515 - Snort Reference ID 54452,54453 (Added)
- CVE: 2020-13516 - Snort Reference ID 54454,54455 (Added)
- CVE: 2020-13517 - Snort Reference ID 54456,54457 (Added)
- CVE: 2020-13518 - Snort Reference ID 54458,54459 (Added)

- CVE: 2020-13519 - Snort Reference ID 54460,54461 (Added)
- CVE: 2020-13520 - Snort Reference ID 54519,54520 (Added)
- CVE: 2020-13524 - Snort Reference ID 54588,54589 (Added)
- CVE: 2020-13525 - Snort Reference ID 54606,54607,54608 (Added)
- CVE: 2020-13526 - Snort Reference ID 54606,54607,54608 (Added)
- CVE: 2020-13527 - Snort Reference ID 54762,54763,54764,54798,54799,54800 (Added)
- CVE: 2020-13530 - Snort Reference ID 54832 (Added)
- CVE: 2020-13531 - Snort Reference ID 54922,54923 (Added)
- CVE: 2020-13541 - Snort Reference ID 55641,55642,55643,55644,55645,55646 (Added)
- CVE: 2020-13544 - Snort Reference ID 55985,55986 (Added)
- CVE: 2020-13545 - Snort Reference ID 55987,55988 (Added)
- CVE: 2020-13547 - Snort Reference ID 56065,56066 (Added)
- CVE: 2020-13556 - Snort Reference ID 56059,56060 (Added)
- CVE: 2020-13557 - Snort Reference ID 56053,56054 (Added)
- CVE: 2020-13559 - Snort Reference ID 56128,56129 (Added)
- CVE: 2020-13560 - Snort Reference ID 56122,56123 (Added)
- CVE: 2020-13570 - Snort Reference ID 51949,51950 (Added)
- CVE: 2020-13573 - Snort Reference ID 56208 (Added)
- CVE: 2020-13584 - Snort Reference ID 56379,56380,56381,56382 (Added)
- CVE: 2020-15901 - Snort Reference ID 56934,56935,56936,56937 (Added)
- CVE: 2020-17096 - Snort Reference ID 56561,56562 (Added)
- CVE: 2020-17121 - Snort Reference ID 56560 (Added)
- CVE: 2020-17140 - Snort Reference ID 56571 (Added)
- CVE: 2020-17144 - Snort Reference ID 56554 (Added)
- CVE: 2020-17152 - Snort Reference ID 56557,56558 (Added)
- CVE: 2020-17158 - Snort Reference ID 56604 (Added)
- CVE: 2020-17530 - Snort Reference ID 29592,47690 (Added)
- CVE: 2020-26085 - Snort Reference ID 56588,56589,56590,56845,56846 (Added)
- CVE: 2020-26878 - Snort Reference ID 56551 (Added)
- CVE: 2020-26879 - Snort Reference ID 56550 (Added)
- CVE: 2020-27127 - Snort Reference ID 56572,56573 (Added)
- CVE: 2020-27132 - Snort Reference ID 56588,56589,56590 (Added)

- CVE: 2020-27133 - Snort Reference ID 56575,56576 (Added)
- CVE: 2020-27134 - Snort Reference ID 56591 (Added)
- CVE: 2020-27648 - Snort Reference ID 56658,56659 (Added)
- CVE: 2020-35234 - Snort Reference ID 56905 (Added)
- CVE: 2021-1146 - Snort Reference ID 56838 (Added)
- CVE: 2021-1147 - Snort Reference ID 56838 (Added)
- CVE: 2021-1148 - Snort Reference ID 56838 (Added)
- CVE: 2021-1149 - Snort Reference ID 56838 (Added)
- CVE: 2021-1150 - Snort Reference ID 56838 (Added)
- CVE: 2021-1159 - Snort Reference ID 56885 (Added)
- CVE: 2021-1160 - Snort Reference ID 56840 (Added)
- CVE: 2021-1161 - Snort Reference ID 56839 (Added)
- CVE: 2021-1162 - Snort Reference ID 56839 (Added)
- CVE: 2021-1163 - Snort Reference ID 56866 (Added)
- CVE: 2021-1164 - Snort Reference ID 42493 (Added)
- CVE: 2021-1165 - Snort Reference ID 56841 (Added)
- CVE: 2021-1166 - Snort Reference ID 56861 (Added)
- CVE: 2021-1167 - Snort Reference ID 56839 (Added)
- CVE: 2021-1168 - Snort Reference ID 56844 (Added)
- CVE: 2021-1169 - Snort Reference ID 56841 (Added)
- CVE: 2021-1170 - Snort Reference ID 56841 (Added)
- CVE: 2021-1171 - Snort Reference ID 56842 (Added)
- CVE: 2021-1172 - Snort Reference ID 54560,54561 (Added)
- CVE: 2021-1173 - Snort Reference ID 56840 (Added)
- CVE: 2021-1174 - Snort Reference ID 56844 (Added)
- CVE: 2021-1175 - Snort Reference ID 56841 (Added)
- CVE: 2021-1177 - Snort Reference ID 56842 (Added)
- CVE: 2021-1178 - Snort Reference ID 56840 (Added)
- CVE: 2021-1179 - Snort Reference ID 56841 (Added)
- CVE: 2021-1180 - Snort Reference ID 56843 (Added)
- CVE: 2021-1181 - Snort Reference ID 56842 (Added)
- CVE: 2021-1182 - Snort Reference ID 56844 (Added)

- CVE: 2021-1183 - Snort Reference ID 56866 (Added)
- CVE: 2021-1184 - Snort Reference ID 56868 (Added)
- CVE: 2021-1185 - Snort Reference ID 56842 (Added)
- CVE: 2021-1186 - Snort Reference ID 56869 (Added)
- CVE: 2021-1187 - Snort Reference ID 56843 (Added)
- CVE: 2021-1188 - Snort Reference ID 56841 (Added)
- CVE: 2021-1189 - Snort Reference ID 56867 (Added)
- CVE: 2021-1190 - Snort Reference ID 56839 (Added)
- CVE: 2021-1191 - Snort Reference ID 56861 (Added)
- CVE: 2021-1192 - Snort Reference ID 56840 (Added)
- CVE: 2021-1193 - Snort Reference ID 56871,56872,56873,56874,56875 (Added)
- CVE: 2021-1194 - Snort Reference ID 56839 (Added)
- CVE: 2021-1195 - Snort Reference ID 56843 (Added)
- CVE: 2021-1196 - Snort Reference ID 56839 (Added)
- CVE: 2021-1197 - Snort Reference ID 56844 (Added)
- CVE: 2021-1198 - Snort Reference ID 56844 (Added)
- CVE: 2021-1199 - Snort Reference ID 56842 (Added)
- CVE: 2021-1200 - Snort Reference ID 56876 (Added)
- CVE: 2021-1201 - Snort Reference ID 56870 (Added)
- CVE: 2021-1202 - Snort Reference ID 56842 (Added)
- CVE: 2021-1203 - Snort Reference ID 56842 (Added)
- CVE: 2021-1204 - Snort Reference ID 56844 (Added)
- CVE: 2021-1205 - Snort Reference ID 56841,56868 (Added)
- CVE: 2021-1206 - Snort Reference ID 56841 (Added)
- CVE: 2021-1207 - Snort Reference ID 56841 (Added)
- CVE: 2021-1209 - Snort Reference ID 56840 (Added)
- CVE: 2021-1210 - Snort Reference ID 56876 (Added)
- CVE: 2021-1211 - Snort Reference ID 56841 (Added)
- CVE: 2021-1212 - Snort Reference ID 56839 (Added)
- CVE: 2021-1213 - Snort Reference ID 56861 (Added)
- CVE: 2021-1214 - Snort Reference ID 56840 (Added)
- CVE: 2021-1215 - Snort Reference ID 56839 (Added)

- CVE: 2021-1216 - Snort Reference ID 56840 (Added)
- CVE: 2021-1217 - Snort Reference ID 56840 (Added)
- CVE: 2021-1237 - Snort Reference ID 56893,56894 (Added)
- CVE: 2021-1258 - Snort Reference ID 56881,56882,56883,56884 (Added)
- CVE: 2021-1647 - Snort Reference ID 56857,56858,56859,56860 (Added)
- CVE: 2021-1707 - Snort Reference ID 56865 (Added)
- CVE: 2021-1709 - Snort Reference ID 56849,56850,56851,56852,56853,56854,56855,56856 (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.