Release Notes for Cisco Vulnerability Database (VDB) Update 339

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 339

Cisco Vulnerability Database (VDB) Update 339 supports 3,593 applications.

Vulnerability Database Update 339 Changelog

This section describes the changes from VDB 338 (1:00:29 PM on September 24th, 2020 UTC) to VDB 339 (9:41:10 PM on November 5th, 2020 UTC).

Application Protocol Detectors

Total Added:	9
Total Removed:	0
Total Updated	3

Client Detectors

Total Added:	0
Total Removed:	0
Total Updated	2

Web Application Detectors

Total Added:	8
Total Removed:	1
Total Updated	48

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:	141
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	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:

- DLMS-COSEM: (Device Language Message Specification) / COSEM (CompanionSpecification for Energy Metering) specifies an interface model and communication protocols for data exchange with metering equipment. (Added)
- DLMS-COSEM Get Response: A DLMS-COSEM service to send a response to a previously received GET indication primitive. (Added)
- DLMS-COSEM Set Response: A DLMS-COSEM service to send a response to a previously received SET indication primitive. (Added)
- DLMS-COSEM Get Request: A DLMS-COSEM service request to get the value(s) of one or all attributes. (Added)
- DLMS-COSEM Set Request: A DLMS-COSEM service request to set the value of one or more attributes. (Added)
- DLMS-COSEM Initiate Response: A DLMS-COSEM service response for User-Information exchange. (Added)
- DLMS-COSEM Initiate Request No Authentication: A DLMS-COSEM service request for User-Information exchange with No Authentication. (Added)

- DLMS-COSEM Initiate Request Low-Level Authentication: A DLMS-COSEM service request for User-Information exchange with Low-Level Authentication. (Added)
- DLMS-COSEM Initiate Request High-Level Authentication: A DLMS-COSEM service request for User-Information exchange with High-Level Authentication. (Added)
- TCX related services (TCX Flash, TCX Multimedia, TCX Sound and TCX USB): Updated detectors to correctly classify TCX traffic flows as some flows were recognized as STUN. (Updated)
- SSL, HTTPS: Enhanced the memory usage while extracting the TLS ja3 attribute. (Updated)
- SSH: Updated detector to classify flows properly. (Updated)

Client Detectors:

- Ultrasurf: Adding support for Ultrasurf app version 20.03 (Updated)
- Telegram: Updated patterns to fix false positives from SSL traffic. (Updated)

Web Application Detectors:

- Xbox Live: Modified detection patterns. (Updated)
- GMX Mail: Modified detection patterns to cover patterns for several geographical domains of GMX website. (Updated)
- GMX: Free webmail and email service provider. (Removed)
- Twitter: Updated patterns to fix false positives from TwitPic traffic. (Updated)
- Ybrant Digital: Updated patterns to fix false positives from Lycos traffic. (Updated)
- Apache Nutch: Updated patterns to fix false positives from Tinder traffic. (Updated)
- Amazon: Updated patterns to fix false positives from AWS traffic. (Updated)
- Aggregate Knowledge: Updated patterns to fix false positives from Neustar Information Services traffic. (Updated)
- Office 365: Updated patterns to fix false positives from Microsoft Azure traffic. (Updated)
- Microsoft CRM Dynamics: Updated patterns to fix false positives from Office 365 traffic. (Updated)
- Tencent Cloud: Updated patterns to fix false positives from WeChat traffic. (Updated)
- Webex Teams: Updated patterns to fix false positives from Cisco Jabber traffic and cover other missed detection. (Updated)
- Taobao: Updated patterns to fix false positives from Tmall traffic. (Updated)
- Alisoft: Updated patterns to fix false positives from Leadbolt traffic. (Updated)
- Woopra: Updated patterns to fix false positives from Disqus traffic. (Updated)
- CNET TV: Updated patterns to fix false positives from Cnet website traffic. (Updated)
- Alibaba: Updated patterns to fix false positives from Taobao website traffic. (Updated)
- Google Ads: Updated patterns to fix false positives from Doubleclick traffic. (Updated)
- BBC iPlayer: Updated patterns to fix false positives from BBC website traffic. (Updated)

- Soso: Updated patterns to fix false positives from Sogou website traffic. (Updated)
- Lord & Taylor: Updated patterns to fix false positives from Saks Fifth Avenue website traffic. (Updated)
- People.com: Updated patterns to fix false positives from TIME.com website traffic. (Updated)
- Entertainment Weekly: Updated patterns to fix false positives from TIME.com website traffic. (Updated)
- Aliwangwang: Updated patterns to fix false positives from Taobao website traffic. (Updated)
- ibVPN Login: Updated patterns to fix false positives from ibVPN website traffic. (Updated)
- GTA Online: Updated patterns to fix false positives from Rockstar Games traffic. (Updated)
- Myspace: Updated patterns to distinguish detection between Myspace, Myspace Photos and Myspace Videos (Updated)
- YiXin: Updated patterns to fix false positives from Netease traffic. (Updated)
- Crackle Video: Updated patterns to fix false positives from Crackle website traffic. (Updated)
- Hulu Video: Updated patterns to fix false positives from Hulu website traffic. (Updated)
- CC Studios: Updated patterns to fix false positives from Comedy Central website traffic. (Updated)
- Netflix Stream: Updated patterns to fix false positives from Netflix website traffic. (Updated)
- Zynga: Updated patterns to distinguish traffic from Words With Friends. (Updated)
- T Mobile: Updated patterns to fix false positives from Advertising.com traffic. (Updated)
- Facebook: Updated patterns to distinguish detection between Facebook Video, Facebook Photos and Facebook (Updated)
- Alibaba: Updated patterns to fix false positives from Alipay traffic. (Updated)
- F-secure: Updated patterns to avoid causing false positives for Malwarebytes. (Updated)
- Windows Live Skydrive: Updated patterns to fix false positives from OneDrive traffic. (Updated)
- Power BI: Updated description and enhanced detection. (Updated)
- Microsoft Teams: Enhanced coverage to include UDP traffic (Updated)
- Azure Service Bus: Azure Service Bus is a multi-tenant cloud messaging service you can use to send information between applications and services. (Added)
- Fiserv: Fiserv is a provider of technology solutions to the financial world, including banks, credit unions, securities processing organizations, insurance companies, etc. (Added)
- Jaspersoft: Jaspersoft embedded analytics software is a BI platform to design, embed, and manage reports and analytics with programmatic control. (Added)
- QlikView: QlikView is a BI data discovery product for creating guided analytics applications and dashboards tailor-made for business challenges. (Added)
- RingCentral: RingCentral is an American publicly traded provider of cloud-based communications and collaboration solutions for businesses. (Added)
- Tableau: Tableau Software is an interactive data visualization and data analytics software which provides pictorial and graphical representations of data. (Added)

- VPN Monster: VPN Monster is a Russia-based VPN service provider that provides its users with a significant degree of anonymity and security. (Added)
- OneLogin: A cloud-based identity and access management service. (Added)
- Smartsheet: Corrected patterns for detection (Updated)
- Jira: Modified application name to lower case and added patterns for detection. (Updated)
- Box: Removed unused patterns (Updated)
- Showbox: Removed unused patterns (Updated)
- ServiceNow: Updated patterns to fix false positives from OneLogin traffic. (Updated)
- QQ Games: Corrected patterns for detection (Updated)
- Google Hangouts: Updated detector to classify flows properly (Updated)
- Google: Updated patterns to fix false positives from Facebook traffic. (Updated)
- Imo.im: Detector updated as some SMTP and SMB flows were getting classified as imo.im. (Updated)

FireSIGHT/Firepower Detector Updates:

- no additions or modifications

File Type Detector Details:

- POSIX_TAR POSIX Tape Archive file – Updated patterns (Updated)

Snort ID Vulnerability Reference Details:

- CVE: 2010-1119 - Snort Reference ID 29623,18958,18957,56042 (Added)
- CVE: 2015-6098 - Snort Reference ID 36745,36744,55198,55197 (Added)
- CVE: 2017-6331 - Snort Reference ID 55814,55813 (Added)
- CVE: 2018-15959 - Snort Reference ID 56151,56150 (Added)
- CVE: 2018-4314 - Snort Reference ID 56044,56043 (Added)
- CVE: 2018-4416 - Snort Reference ID 56009,56008 (Added)
- CVE: 2018-4939 - Snort Reference ID 56151,56150 (Added)
- CVE: 2018-9995 - Snort Reference ID 46826,46825,55840,55839 (Added)
- CVE: 2019-0230 - Snort Reference ID 41923,41922 (Added)
- CVE: 2019-0233 - Snort Reference ID 56001,56000,55999 (Added)
- CVE: 2019-0604 - Snort Reference ID 51368,49861,50275,55862 (Added)
- CVE: 2019-13372 - Snort Reference ID 55981 (Added)
- CVE: 2019-13373 - Snort Reference ID 56002 (Added)
- CVE: 2019-13374 - Snort Reference ID 56004 (Added)
- CVE: 2019-13375 - Snort Reference ID 56007,56006,56005 (Added)

- CVE: 2019-15283 - Snort Reference ID 52102,52103 (Added)
- CVE: 2019-15285 - Snort Reference ID 52106,52107 (Added)
- CVE: 2019-15287 - Snort Reference ID 52110,52111 (Added)
- CVE: 2019-15957 - Snort Reference ID 52119,52120,52121,52122 (Added)
- CVE: 2019-15993 - Snort Reference ID 52993,52994,52995,52996,52997 (Added)
- CVE: 2019-16009 - Snort Reference ID 52559,52560 (Added)
- CVE: 2019-16019 - Snort Reference ID 52633 (Added)
- CVE: 2019-16021 - Snort Reference ID 52633 (Added)
- CVE: 2019-16023 - Snort Reference ID 52633 (Added)
- CVE: 2019-16028 - Snort Reference ID 52627,52628,52629,52630,52631 (Added)
- CVE: 2019-1888 - Snort Reference ID 53168 (Added)
- CVE: 2019-1983 - Snort Reference ID 53170 (Added)
- CVE: 2019-8762 - Snort Reference ID 55799,55798 (Added)
- CVE: 2019-9670 - Snort Reference ID 49865,49864 (Added)
- CVE: 2020-0664 - Snort Reference ID 55140,55139 (Added)
- CVE: 2020-0856 - Snort Reference ID 55206 (Added)
- CVE: 2020-0941 - Snort Reference ID 55188,55187 (Added)
- CVE: 2020-1115 - Snort Reference ID 55142,55141 (Added)
- CVE: 2020-1152 - Snort Reference ID 55162,55161 (Added)
- CVE: 2020-1170 - Snort Reference ID 55922 (Added)
- CVE: 2020-1245 - Snort Reference ID 55144,55143 (Added)
- CVE: 2020-1308 - Snort Reference ID 55146,55145 (Added)
- CVE: 2020-13499 - Snort Reference ID 54478 (Added)
- CVE: 2020-13500 - Snort Reference ID 54478 (Added)
- CVE: 2020-13501 - Snort Reference ID 54478 (Added)
- CVE: 2020-13504 - Snort Reference ID 54480 (Added)
- CVE: 2020-13505 - Snort Reference ID 54480 (Added)
- CVE: 2020-13699 - Snort Reference ID 54995,54994 (Added)
- CVE: 2020-13934 - Snort Reference ID 55801,55800 (Added)
- CVE: 2020-13935 - Snort Reference ID 56086 (Added)
- CVE: 2020-14386 - Snort Reference ID 56052,56051 (Added)
- CVE: 2020-14644 - Snort Reference ID 55933,55932 (Added)

- CVE: 2020-1472 - Snort Reference ID 55704,55703,55802 (Added)
- CVE: 2020-15363 - Snort Reference ID 55838,55837,55836 (Added)
- CVE: 2020-15364 - Snort Reference ID 55835,55834 (Added)
- CVE: 2020-15505 - Snort Reference ID 56155,56154 (Added)
- CVE: 2020-16875 - Snort Reference ID 55826 (Added)
- CVE: 2020-16896 - Snort Reference ID 55994 (Added)
- CVE: 2020-16898 - Snort Reference ID 55984 (Added)
- CVE: 2020-16899 - Snort Reference ID 55993 (Added)
- CVE: 2020-16907 - Snort Reference ID 55943,55942 (Added)
- CVE: 2020-16913 - Snort Reference ID 55990,55989 (Added)
- CVE: 2020-16915 - Snort Reference ID 55980,55979 (Added)
- CVE: 2020-16922 - Snort Reference ID 55983,55982 (Added)
- CVE: 2020-16947 - Snort Reference ID 56157,56156 (Added)
- CVE: 2020-16952 - Snort Reference ID 56136,56135,56134,56070,56069 (Added)
- CVE: 2020-17496 - Snort Reference ID 51621,51620,51837,51836,51835 (Added)
- CVE: 2020-25213 - Snort Reference ID 55778 (Added)
- CVE: 2020-3141 - Snort Reference ID 55815,55816,55817 (Added)
- CVE: 2020-3304 - Snort Reference ID 16195 (Added)
- CVE: 2020-3359 - Snort Reference ID 55832 (Added)
- CVE: 2020-3399 - Snort Reference ID 55830 (Added)
- CVE: 2020-3425 - Snort Reference ID 55818 (Added)
- CVE: 2020-3426 - Snort Reference ID 55808 (Added)
- CVE: 2020-3430 - Snort Reference ID 55016,55017,55018,55035 (Added)
- CVE: 2020-3436 - Snort Reference ID 56087 (Added)
- CVE: 2020-3456 - Snort Reference ID 56084,56085 (Added)
- CVE: 2020-3487 - Snort Reference ID 55831,55924,55925 (Added)
- CVE: 2020-3488 - Snort Reference ID 55806 (Added)
- CVE: 2020-3492 - Snort Reference ID 55820 (Added)
- CVE: 2020-3494 - Snort Reference ID 55807 (Added)
- CVE: 2020-3495 - Snort Reference ID 55035 (Added)
- CVE: 2020-3510 - Snort Reference ID 55822 (Added)
- CVE: 2020-3516 - Snort Reference ID 55833 (Added)

- CVE: 2020-3526 - Snort Reference ID 55819 (Added)
- CVE: 2020-3528 - Snort Reference ID 56090,56091 (Added)
- CVE: 2020-3572 - Snort Reference ID 56089 (Added)
- CVE: 2020-3894 - Snort Reference ID 55013,55012 (Added)
- CVE: 2020-4211 - Snort Reference ID 55921,55920,55919,55918 (Added)
- CVE: 2020-6083 - Snort Reference ID 53125 (Added)
- CVE: 2020-6085 - Snort Reference ID 53049 (Added)
- CVE: 2020-6086 - Snort Reference ID 53049,53127 (Added)
- CVE: 2020-6087 - Snort Reference ID 53128 (Added)
- CVE: 2020-6097 - Snort Reference ID 53565 (Added)
- CVE: 2020-6104 - Snort Reference ID 53731,53732 (Added)
- CVE: 2020-6105 - Snort Reference ID 53684,53685 (Added)
- CVE: 2020-6106 - Snort Reference ID 53742,53743 (Added)
- CVE: 2020-6107 - Snort Reference ID 53684,53685 (Added)
- CVE: 2020-6108 - Snort Reference ID 53729,53730 (Added)
- CVE: 2020-6112 - Snort Reference ID 53990,53991 (Added)
- CVE: 2020-6113 - Snort Reference ID 53948,53949 (Added)
- CVE: 2020-6115 - Snort Reference ID 53992,53993 (Added)
- CVE: 2020-6116 - Snort Reference ID 54010,54011 (Added)
- CVE: 2020-6117 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6118 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6119 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6120 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6121 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6122 - Snort Reference ID 54132,54133,54134 (Added)
- CVE: 2020-6123 - Snort Reference ID 54135,54136,54137 (Added)
- CVE: 2020-6124 - Snort Reference ID 54135,54136,54137 (Added)
- CVE: 2020-6125 - Snort Reference ID 54138 (Added)
- CVE: 2020-6126 - Snort Reference ID 54139,54140,54141 (Added)
- CVE: 2020-6127 - Snort Reference ID 54139,54140,54141 (Added)
- CVE: 2020-6128 - Snort Reference ID 54139,54140,54141 (Added)
- CVE: 2020-6129 - Snort Reference ID 54142,54143,54144 (Added)

- CVE: 2020-6130 - Snort Reference ID 54142,54143,54144 (Added)
- CVE: 2020-6131 - Snort Reference ID 54142,54143,54144 (Added)
- CVE: 2020-6132 - Snort Reference ID 54123,54124,54125 (Added)
- CVE: 2020-6133 - Snort Reference ID 54126,54127,54128 (Added)
- CVE: 2020-6134 - Snort Reference ID 54129,54130,54131 (Added)
- CVE: 2020-6135 - Snort Reference ID 54259,54260,54261 (Added)
- CVE: 2020-6136 - Snort Reference ID 54262,54263,54264 (Added)
- CVE: 2020-6137 - Snort Reference ID 54251,54252,54253 (Added)
- CVE: 2020-6138 - Snort Reference ID 54251,54252,54253 (Added)
- CVE: 2020-6139 - Snort Reference ID 54251,54252,54253 (Added)
- CVE: 2020-6140 - Snort Reference ID 54251,54252,54253 (Added)
- CVE: 2020-6141 - Snort Reference ID 54267,54268,54269 (Added)
- CVE: 2020-6142 - Snort Reference ID 54254,54255,54256 (Added)
- CVE: 2020-6143 - Snort Reference ID 54257,54258 (Added)
- CVE: 2020-6144 - Snort Reference ID 54257,54258 (Added)
- CVE: 2020-6146 - Snort Reference ID 54047,54048 (Added)
- CVE: 2020-6151 - Snort Reference ID 54411,54412,54413,54414 (Added)
- CVE: 2020-6152 - Snort Reference ID 54390,54391 (Added)
- CVE: 2020-6388 - Snort Reference ID 55810,55809 (Added)
- CVE: 2020-6967 - Snort Reference ID 55743 (Added)
- CVE: 2020-7047 - Snort Reference ID 55797 (Added)
- CVE: 2020-7048 - Snort Reference ID 55797 (Added)
- CVE: 2020-8163 - Snort Reference ID 55821 (Added)
- CVE: 2020-8193 - Snort Reference ID 56138 (Added)
- CVE: 2020-8195 - Snort Reference ID 56138,56162 (Added)
- CVE: 2020-8218 - Snort Reference ID 55640,55639,55638,55637 (Added)
- CVE: 2020-8758 - Snort Reference ID 55210,55209,55208,55207 (Added)
- CVE: 2020-8844 - Snort Reference ID 55742,55741 (Added)
- CVE: 2020-9496 - Snort Reference ID 55978 (Added)
- CVE: 2020-9609 - Snort Reference ID 53563,53564 (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.