Release Notes for Cisco Cyber Vision Knowledge DB

Release 202112

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 are compatible with this Knowledge DB file.

Links

Software Download

The files listed below can be found using the following link:

https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.0.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.0.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.0.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.0.3.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.0.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.0.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.0.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.0.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4.0.3	**Description**
CiscoCyberVision-Embedded-KDB-4.0.3.dat	Knowledge DB embedded in Cisco Cyber Vision 4.0.3
Updates/KDB/KDB.202112	**Description**
CiscoCyberVision_knowledgedb_20211203.db	Knowledge DB version 20211203
CiscoCyberVision_knowledgedb_20211210.db	Knowledge DB version 20211210
CiscoCyberVision_knowledgedb_20211213.db	Knowledge DB version 20211213
CiscoCyberVision_knowledgedb_20211217.db	Knowledge DB version 20211217
CiscoCyberVision_knowledgedb_20211224.db	Knowledge DB version 20211224
CiscoCyberVision_knowledgedb_20211231.db	Knowledge DB version 20211231

Related Documentation

- Cisco Cyber Vision GUI User Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf

Database download

Cisco Cyber Vision uses an internal database which contains the list of recognized vulnerabilities, icons, threats, etc. Cisco has published a new Knowledge DB for Cisco Cyber Vision. This Knowledge DB (or KDB) is essential for Cisco Cyber Vision. It allows, in particular, the detection of vulnerabilities.

This database can be updated using the file available from the link above. The file contains a built-in RSA signature and external checking is not required; the file will be verified by Cisco Cyber Vision Center at import time.

How to update the database

To update the Knowledge DB:

1. Download the latest DB file available.
2. From the Cisco Cyber Vision system administration page, click the Import a knowledge DB button to upload the file.

Importing the new database will rematch your existing components against any new vulnerabilities.

Release contents

20211231

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-30 (https://www.snort.org/advisories/talos-rules-2021-12-30)**
  - Talos has added and modified multiple rules in the malware-cnc, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211224

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-21 (https://www.snort.org/advisories/talos-rules-2021-12-21)**
  - Talos is releasing updates to Snort SIDs: 58722-58744, 58751, 58784-58790, 58795, 58801, 58811-58814 to address CVE-2021-44228/CVE-2021-45046/CVE-2021-45105, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the file-executable, file-pdf, indicator-compromise, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-12-17 (https://www.snort.org/advisories/talos-rules-2021-12-17)**
  - Talos is releasing updates to Snort SIDs: 58740-58742 and new Snort SIDs: 58801-58814 to address CVE-2021-44228/CVE-2021-45046, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the indicator-obfuscation, malware-cnc, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-45105: (Apache Log4j Vulnerabilities - Uncontrolled Recursion in Siemens Energy Sensformer)
  Apache Log4j2 versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $${ctx:loginId}). This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data that contains a recursive lookup, resulting in a denial of service condition.
- CVE-2021-45046: (Apache Log4j Vulnerabilities - Improper Input Validation in Siemens Energy Sensformer)
  The fix to address CVE-2021-44228 was incomplete in certain non-default configurations, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, ${ctx:loginId}). This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data using a JNDI Lookup pattern, resulting in an information leak and remote code execution in some environments and local code execution in all environments.
- CVE-2021-44228: (Apache Log4j Vulnerabilities - Improper Input Validation in Siemens Energy Sensformer
  Apache Log4j V2, versions < 2.15.0 do not protect JNDI features (as used in configuration, log messages, and parameters) against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters could execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

- CVE-2019-5097: (Loop with Unreachable Exit Condition Vulnerability in Rockwell 1783-NATR through the GoAhead web server)
  A remote unauthenticated attacker may be able to send a specially crafted HTTP request that can lead to an infinite loop in the process. The request can be unauthenticated in the form of GET or POSTS requests and does not require the requested resource on the server, which would lead to a denial-of-service attack on the device.
- CVE-2019-5096: (Use After Free vulnerability in Rockwell 1783-NATR through the GoAhead web server)
  A remote unauthenticated attacker may be able to send a specially crafted HTTP request that can lead to a use-after-free condition during the processing of this request that can be used to corrupt heap structures, which would result in the ability for the attacker to execute remote code execution.
- CVE-2021-44463: (Uncontrolled Search Path Element in DeltaV Distributed Control System Controllers and Workstations)
  Missing DLLs, if replaced by an insider, could allow an attacker to achieve local privilege escalation when some DeltaV services are started.
- CVE-2021-26264: (Missing Authentication for Critical Function in DeltaV Distributed Control System Controllers and Workstations)
  A specially crafted script could cause a controller to restart and cause a denial-of-service condition.
- CVE-2021-35534: (Cleartext Transmission of Sensitive Information in Moxa MGate Protocol Gateways)
  The affected products contain vulnerable firmware, which could allow an attacker to sniff the traffic and decrypt login credential details. This could give an attacker admin rights through the HTTP web server.

20211217

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-15 (https://www.snort.org/advisories/talos-rules-2021-12-15)**
  - Talos is releasing updates to Snort 2 SIDs: 58722-58744, 58751, 58784-58790 and a new Snort 2 SID: 58795 to address CVE-2021-44228/CVE-2021-45046, an RCE vulnerability in the Apache Log4j API.
  - Talos also has added and modified multiple rules in the malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-12-14 (https://www.snort.org/advisories/talos-rules-2021-12-14)**
  - Microsoft Vulnerability CVE-2021-41333: A coding deficiency exists in Microsoft Windows Print Spooler that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58752 through 58753.
  - Microsoft Vulnerability CVE-2021-43207: A coding deficiency exists in Microsoft Windows Common Log File System driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58775 through 58776.
  - Microsoft Vulnerability CVE-2021-43226: A coding deficiency exists in Microsoft Windows Common Log File System driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58754 through 58757.

- Microsoft Vulnerability CVE-2021-43233: A coding deficiency exists in Remote Desktop Client that may lead to remote code execution.
- A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 58774.
- Microsoft Vulnerability CVE-2021-43883: A coding deficiency exists in Microsoft Windows Installer that may lead to an escalation of privilege.
- Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 58635 through 58636.
- Talos is releasing updates to Snort 2 SIDs: 58740-58741 and new Snort 2 SIDs: 58784-58790 to address CVE-2021-44228, an RCE vulnerability in the Apache Log4j API.
- Talos has also added and modified multiple rules in the file-pdf, malware-cnc, malware-other, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2021-12-13 (https://www.snort.org/advisories/talos-rules-2021-12-13)**
  - Talos is releasing updates to Snort 2 SIDs: 58740-58744 and Snort 3 SID: 300058, as well as a new Snort 2 SID: 58751 to address CVE-2021-44228, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the file-multimedia and server-webapp rule sets to provide coverage for emerging threats from these technologies.

Concerning Log4j Snort rules

- The majority of the Log4j rules that were exclusively in the Subscriber Snort ruleset in the Knowledge DB version 20211213 are now also included in the Community (free) Snort ruleset.
- The Subscriber ruleset contains nine new Log4j Snort rules that are currently not in the Community ruleset. The SIDs of these rules are detailed in the Talos advisories mentioned above.

This release also adds support and modifications for the detection of the following vulnerabilities:

- CVE-2021-44165: (Remote Code Execution Vulnerability in Siemens POWER METER SICAM Q100)
  The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin privileges to potentially perform remote code execution.
- CVE-2021-22825: (Improper Neutralization of Input During Web Page Generation In Schneider Rack Power Distribution Unit)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an attacker to access the system with elevated privileges when a privileged account clicks on a malicious URL that compromises the security token.
- CVE-2021-22724: (Cross-Site Request Forgery (CSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent to the charging station web server.
- CVE-2021-22725: (Cross-Site Request Forgery (CSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could cause allow an attacker to

perform unintended actions when crafted malicious parameters are submitted in GET requests sent to the charging station web server.

- CVE-2021-22818: (Improper Restriction of Excessive Authentication Attempts in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to gain unauthorized access to the charging station web interface by performing brute force attacks.
- CVE-2021-22819: (Improper Restriction of Rendered UI Layers or Frames in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the web interface rendered within iframes.
- CVE-2021-22820: (Insufficient Session Expiration in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-614 Insufficient Session Expiration vulnerability exists that could allow an attacker to maintain an unauthorized access over a hijacked session to the charger station web server even after the legitimate user account holder has changed his password.
- CVE-2021-22821: (Server-Side Request Forgery (SSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-918 Server-Side Request Forgery (SSRF) vulnerability exists that could cause the station web server to forward requests to unintended network targets when crafted malicious parameters are submitted to the charging station web server.
- CVE-2021-22822: (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.
- CVE-2021-42027: (Improper Certificate Validation Vulnerability in Siemens SINUMERIK Edge)
  The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server.
- CVE-2019-15690: (Integer Overflow or Wraparound in LibVNCServer)
  A flaw was found in libvncserver. An integer overflow within the HandleCursorShape() function can be exploited to cause a heap-based buffer overflow by tricking a user or application using libvncserver to connect to an unstrusted server and subsequently send cursor shapes with specially crafted dimensions. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
- CVE-2018-20750: (Out-of-bounds Write in LibVNCServer)
  LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
- CVE-2020-14398: (Loop with Unreachable Exit Condition in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c.
- CVE-2020-14397: (NULL Pointer Dereference in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has a NULL pointer

dereference.

- CVE-2019-15681: (Improper Initialization in LibVNC)
  LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.
- CVE-2020-14402: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings.
- CVE-2017-18922: (Out-of-bounds Write in LibVNC)
  websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A malicious attacker could exploit this by sending specially crafted WebSocket frames to a server, causing a heap-based buffer overflow.
- CVE-2020-14404: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings.
- CVE-2019-20788: (Integer Overflow or Wraparound in LibVNCServer)
  libvncclient/cursor.c in LibVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.
- CVE-2020-14403: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via encodings.
- CVE-2019-15690: (Integer Overflow or Wraparound in LibVNCServer)
  A flaw was found in libvncserver. An integer overflow within the HandleCursorShape() function can be exploited to cause a heap-based buffer overflow by tricking a user or application using libvncserver to connect to an unstrusted server and subsequently send cursor shapes with specially crafted dimensions. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
- CVE-2018-20748: (Out-of-bounds Write in LibVNC)
  LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c. The fix for CVE-2018-20019 was incomplete.
- CVE-2020-14396: (NULL Pointer Dereference in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference.
- CVE-2019-20840: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/ws_decode.c can lead to a crash because of unaligned accesses in hybiReadAndDecode.
- CVE-2019-20839: (Buffer Copy without Checking Size of Input in LibVNCServer)
  libvncclient/sockets.c in LibVNCServer before 0.9.13 has a buffer overflow via a long socket filename.
- CVE-2020-14401: (Integer Overflow or Wraparound in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow.
- CVE-2018-21247: (Exposure of Sensitive Information to an Unauthorized Actor in LibVNCClient)
  An issue was discovered in LibVNCServer before 0.9.13. There is an information leak (of uninitialized

memory contents) in the libvncclient/rfbproto.c ConnectToRFBRepeater function.

- CVE-2018-20749: (Out-of-bounds Write in LibVNCServer)
  LibVNC before 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
- CVE-2018-20019: (Out-of-bounds Write in LibVNC)
  LibVNC before commit a83439b9fbe0f03c48eb94ed05729cb016f8b72f contains multiple heap out-of-bound write vulnerabilities in VNC client code that can result remote code execution.
- CVE-2020-14405: (Allocation of Resources Without Limits or Throttling in LibVNCClient)
  An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size.

20211213

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-11 (https://www.snort.org/advisories/talos-rules-2021-12-11)**
  - Talos is releasing Snort 2 SIDs: 58740-58744 and Snort 3 SID: 300058 to address CVE-2021-44228, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-12-10 (https://www.snort.org/advisories/talos-rules-2021-12-10-12-11-2021)**
  - Talos is releasing updates to SIDs 58726, 58730, 58732 and six new SIDs 58734-58739 to address CVE-2021-44228, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-12-10 (https://www.snort.org/advisories/talos-rules-2021-12-10)**
  - Talos is releasing Snort 2 SIDs 58722-58733 and Snort 3 SIDs: 300055-300057 to address CVE-2021-44228, an RCE vulnerability in the Apache Log4j API.
  - Talos has added and modified multiple rules in the server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211210

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-09 (https://www.snort.org/advisories/talos-rules-2021-12-09)**
  - Talos has added and modified multiple rules in the browser-ie, browser-other, file-multimedia, file-office, file-other, file-pdf, malware-cnc, malware-other, os-windows, policy-other, protocol-scada and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-12-07 (https://www.snort.org/advisories/talos-rules-2021-12-07)**
  - In this release a number of rules have been added to the security policy as part of ongoing policy rebalancing efforts.
  - Talos has added and modified multiple rules in the app-detect, browser-firefox, browser-ie, browser-plugins, browser-webkit, exploit-kit, file-flash, file-image, file-multimedia, file-office, file-other, file-pdf,

malware-cnc, malware-other, netbios, os-mobile, os-other, os-solaris, os-windows, policy-other, protocol-dns, protocol-rpc, protocol-scada, protocol-snmp, protocol-telnet, protocol-tftp, server-apache, server-mail, server-mysql, server-oracle, server-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20211203

This release includes additions to the Snort ruleset covering the following Talos advisories:

- **Talos Rules 2021-12-02 (https://www.snort.org/advisories/talos-rules-2021-12-02)**
  - Talos has added and modified multiple rules in the browser-chrome, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-11-30 (https://www.snort.org/advisories/talos-rules-2021-11-30)**
  - Talos has added and modified multiple rules in the file-other, file-pdf, malware-cnc, os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.