Release Notes for Cisco Cyber Vision Knowledge DB

Release 202205

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-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202205	**Description**
CiscoCyberVision_knowledgedb_20220506.db	Knowledge DB version 20220506
CiscoCyberVision_knowledgedb_20220513.db	Knowledge DB version 20220513
CiscoCyberVision_knowledgedb_20220520.db	Knowledge DB version 20220520
CiscoCyberVision_knowledgedb_20220525.db	Knowledge DB version 20220525

Related Documentation

- Cisco Cyber Vision GUI User Guide:

  https://www.cisco.com/c/en/us/td/docs/security/cyber_vision/publications/GUI/b_Cisco_Cyber_Vision_GUI_User_Guide.html

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

20220525

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

- **Talos Rules 2022-05-24 (https://www.snort.org/advisories/talos-rules-2022-05-24)**
  - Talos has added and modified multiple rules in the file-image, file-multimedia, file-other, malware-cnc, os-linux, os-windows, policy-other, protocol-dns, server-mail, server-oracle 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-2022-1797: (Uncontrolled Resource Consumption in Rockwell Automation Logix Controllers)
  - A malformed Class 3 common industrial protocol message with a cached connection can cause a denial-of-service condition, resulting in a major nonrecoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online.

20220520

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

- **Talos Rules 2022-05-19 (https://www.snort.org/advisories/talos-rules-2022-05-19)**
  - Talos has added and modified multiple rules in the os-windows and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-05-17 (https://www.snort.org/advisories/talos-rules-2022-05-17)**
  - Talos has added and modified multiple rules in the file-image, file-multimedia, file-other, file-pdf, malware-other, policy-other, protocol-imap, protocol-scada, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220513

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

- **Talos Rules 2022-05-12 (https://www.snort.org/advisories/talos-rules-2022-05-12)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, policy-other, protocol-dns, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-05-10 (https://www.snort.org/advisories/talos-rules-2022-05-10)**
  - Microsoft Vulnerability CVE-2022-23270: A coding deficiency exists in Point-to-Point Tunneling Protocol 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 59726 for Snort2, and GID 1, SID 300125 for Snort3.
  - Microsoft Vulnerability CVE-2022-23279: A coding deficiency exists in Microsoft Windows ALPC 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 59727 through 59728 for Snort2, and GID 1, SID 300126 for Snort3.

- Microsoft Vulnerability CVE-2022-26925: A coding deficiency exists in Microsoft Windows LSA that may lead to spoofing.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 59737 for Snort2, and GID 1, SID 300133 for Snort3.
- Microsoft Vulnerability CVE-2022-26937: A coding deficiency exists in Microsoft Windows Network File System that may lead to remote code execution.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 59738 through 59741 for Snort2, and GID 1, SIDs 300134 through 300137 for Snort3.
- Microsoft Vulnerability CVE-2022-29104: 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 59730 through 59731 for Snort2 and GID 1, SID 300128 for Snort3..
- Microsoft Vulnerability CVE-2022-29142: A coding deficiency exists in Microsoft Windows Kernel 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 59733 through 59734 for Snort2, and GID 1, SIDs 300129 through 300130 for Snort3.
- Talos also has added and modified multiple rules in the file-image, file-java, malware-cnc, os-windows, policy-other, protocol-dns, protocol-rpc, protocol-voip 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-2022-24043: (Observable Discrepancy Vulnerability in Siemens PXC and DXR Devices)
    - The login functionality of the application fails to normalize the response times of login attempts performed with wrong usernames with the ones executed with correct usernames. A remote unauthenticated attacker could exploit this side-channel information to perform a username enumeration attack and identify valid usernames.
- CVE-2021-22901: (Use After Free Vulnerability in Siemens Industrial devices using libcurl)
    - libcurl 7.75.0 through 7.76.1 suffers from a use-after-free vulnerability resulting in already freed memory being used when a TLS 1.3 session ticket arrives over a connection. A malicious attacker can use this to reach remote code execution in the client. When libcurl at run-time sets up support for TLS 1.3 session tickets on a connection using OpenSSL, it stores pointers to the transfer in-memory object for later retrieval when a session ticket arrives. If the connection is used by multiple transfers (as with a reused HTTP/1.1 connection or multiplexed HTTP/2 connection) that first transfer object might be freed before the new session is established and the function will then access a memory buffer that might be freed. When using that memory, libcurl may call a function pointer in the object, making it possible for remote code execution if the server could manage to get crafted memory content into the correct place in memory.
- CVE-2022-24042: (Insufficient Session Expiration Vulnerability in Siemens PXC and DXR Devices)
    - The web application returns an AuthToken that does not expire at the defined auto logoff delay timeout. An attacker could capture this token and re-use old session credentials or session IDs for authorization.
- CVE-2022-24040: (Uncontrolled Resource Consumption Vulnerability in Siemens PXC and DXR Devices)

  - The web application fails to enforce an upper bound to the cost factor of the PBKDF2 derived key during the creation or update of an account. An attacker with the user profile access privilege could cause a denial-of-service condition through CPU consumption by setting a PBKDF2 derived key with a high-cost effort, followed by a login attempt to the modified account.

- CVE-2021-41545: (Uncaught Exception Vulnerability in Siemens PXC and DXR Devices)
  - When the controller receives a specific BACnet protocol packet, an exception causes the BACnet communication function to go into a "out of work" state and could result in the controller going into a "factory reset" state.
- CVE-2022-24045: (Sensitive Cookie in HTTPS Session Without 'Secure' Attribute Vulnerability in Siemens PXC and DXR Devices)
  - Following a successful login, the application sets the session cookie on the browser via client-side JavaScript code without applying security attributes (such as "Secure" "HttpOnly" or "SameSite"). Any attempts to browse the application via unencrypted HTTP protocol would lead to the transmission of all session cookies in plaintext through the network. An attacker could then sniff the network and capture sensitive information.
- CVE-2022-24039: (Special Element Injection Vulnerability in Siemens PXC and DXR Devices)
  - The "addCell" JavaScript function fails to properly sanitize user-controllable input before including it into the generated XML body of the XLS report document as it is possible to inject arbitrary content (e.g., XML tags) into the generated file. An attacker with restricted privileges could corrupt the content used to generate XLS reports to leverage the application to deliver malicious files against higher-privileged users and obtain remote code execution (RCE) against the administrator's workstation.
- CVE-2021-22924: (Use After Free Vulnerability in Siemens Industrial devices using libcurl)
  - libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. Due to errors in the logic, the config matching function did not take 'issuercert' into account and compares the involved paths case insensitively, which could lead to libcurl reusing wrong connections. File paths are, or can be, case sensitive on many systems and can vary depending on used file systems. The comparison also didn't include the 'issuer cert,' which a transfer can set to qualify how to verify the server certificate.
- CVE-2022-24044: (Improper Restriction of Excessive Authentication Attempts Vulnerability in Siemens PXC and DXR Devices)
  - The login functionality of the application does not employ countermeasures against password spraying attacks or credential stuffing attacks. An attacker could obtain a list of valid usernames on the device and use that list to perform a precise password spraying or credential stuffing attack to obtain access to at least one account.
- CVE-2022-27640: (Uncontrolled Resource Consumption Vulnerability in Siemens SIMATIC CP 442-1 RNA)
  - The affected devices improperly handle excessive ARP broadcast requests. This could allow an attacker to create a denial-of-service condition by performing ARP storming attacks, which can cause the device to reboot.
- CVE-2022-24041: (Use of Password Hash with Insufficient Computational Effort Vulnerability in Siemens PXC and DXR Devices)
  - The web application stores the PBKDF2 derived key of user's passwords with a low iteration count. An attacker with user profile access privilege can retrieve the stored password hashes of other accounts

and then successfully perform an offline cracking attack and recover the plaintext passwords of other users.

20220506

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

- **Talos Rules 2022-05-05 (https://www.snort.org/advisories/talos-rules-2022-05-05)**
    - Talos has added and modified multiple rules in the file-image, os-other, protocol-ftp, server-mysql and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-05-03 (https://www.snort.org/advisories/talos-rules-2022-05-03)**
    - Talos has added and modified multiple rules in the file-image 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-2015-0248: (Resource Management Errors in Yokogawa CENTUM and ProSafe-RS)
    - The AD suite version management function is subjected to malformed packets, which the functions provided by the AD server may stop.
- CVE-2018-11782: (Improper Input Validation Vulnerability in Yokogawa CENTUM and ProSafe-RS)
    - The AD suite version management function is subjected to malformed packets, which the functions provided by the AD server may stop.
- CVE-2019-0203: (Null Pointer Dereference Vulnerability in Yokogawa CENTUM and ProSafe-RS)
    - The AD suite version management function is subjected to malformed packets, which the functions provided by the AD server may stop.
- CVE-2022-27188: (OS Command Injection Vulnerability in Yokogawa CENTUM and ProSafe-RS)
    - A local attacker could tamper with files generated by the graphic builder, which may allow arbitrary programs to be executed on a computer that has installed standard operation and monitoring function (HIS).
- CVE-2022-26034: (Improper Authentication Vulnerability in Yokogawa CENTUM and ProSafe-RS)
    - Improper authentication of the communication protocol provided by the Automation Design (AD) server allows an attacker to use the functions provided by the AD server. This may lead to leakage or tampering of data managed by the AD server.