Release Notes for Cisco Cyber Vision Knowledge DB

Release 202311

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-4.2.6.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.6.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.6.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.6.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.6.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.6.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.6.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.6.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.6.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.6
Updates/KDB/KDB.202311	**Description**
CiscoCyberVision_knowledgedb_20231103.db	Knowledge DB version 20231103
CiscoCyberVision_knowledgedb_20231110.db	Knowledge DB version 20231110
CiscoCyberVision_knowledgedb_20231117.db	Knowledge DB version 20231117
CiscoCyberVision_knowledgedb_20231124.db	Knowledge DB version 20231124

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

20231124

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

- **Talos Rules 2023-11-21 (https://www.snort.org/advisories/talos-rules-2023-11-21)**
- **Talos Rules 2023-11-16 (https://www.snort.org/advisories/talos-rules-2023-11-16)**

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SIDs 300762
- 1 malware-cnc rule with SIDs 62670
- 1 malware-other rule with SIDs 300761
- 2 protocol-other rules with SIDs 62655, 62656
- 7 server-webapp rules with SIDs 62650, 300759, 300760, 62654, 62649, 62653, 62648

20231117

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

- **Talos Rules 2023-11-14 (https://www.snort.org/advisories/talos-rules-2023-11-14)**

The new and updated Snort rules span the following categories:

- 1 file-office rules with SID 300758
- 1 malware-cnc rules with SID 62647
- 5 os-windows rules with SIDs 300753, 300757, 62626, 300751, 300752
- 1 server-oracle rules with SID 300750
- 6 server-webapp rules with SIDs 62640, 62629, 300756, 62555, 300755, 300754

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

- CVE-2022-47522: (Wi-Fi Encryption Bypass Vulnerabilities in SCALANCE W700 Product Family)
  - The IEEE 802.11 specifications through 802.11ax allow physically proximate attackers to intercept (possibly cleartext) target-destined frames by spoofing a target's MAC address, sending Power Save frames to the access point, and then sending other frames to the access point (such as authentication frames or re-association frames) to remove the target's original security context. This behavior occurs because the specifications do not require an access point to purge its transmit queue before removing a client's pairwise encryption key.
- CVE-2022-44792: (NULL Pointer Dereference Vulnerability in Siemens MV500)

  - handle_ipDefaultTTL in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.8 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker (who has write access) to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service

- CVE-2022-23219: (Classic Buffer Overflow Vulnerability in Siemens MV500)
  - The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.
- CVE-2022-23218: (Classic Buffer Overflow Vulnerability in Siemens MV500)
  - The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.
- CVE-2022-44793: (NULL Pointer Dereference Vulnerability in Siemens MV500)
  - handle_ipv6IpForwarding in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.4.3 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
- CVE-2023-2975: (Improper Authentication Vulnerability in Siemens MV500)
  - The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be mislead by removing adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue
- CVE-2023-35788: (Out-of-bounds Write Vulnerability in Siemens MV500)
  - An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-bounds write in the flower classifier code via TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in denial of service or privilege escalation.
- CVE-2023-3817: (Excessive Iteration Vulnerability in Siemens MV500)
  - Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of

Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check().

- CVE-2023-3446: (Inefficient Regular Expression Complexity Vulnerability in Siemens MV500)
    - Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option.
- CVE-2023-4203: (Out-of-bounds Read Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial-of-service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.
- CVE-2023-4304: (Inadequate Encryption Strength Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - A timing-based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial

messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

- CVE-2023-4450: (Double Free Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the “name” (e.g. “CERTIFICATE"), any header data and the payload data. If the function succeeds then the “name_out”, “header” and “data” arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer, then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial-of-service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable.
- CVE-2023-44374: (Improper Synchronization Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices allow to change the password, but insufficiently check which password is to be changed. With this an authenticated attacker could, under certain conditions, be able to change the password of another, potential admin user allowing her to escalate her privileges
- CVE-2023-44320: (Forced Browsing Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices do not properly validate the authentication when performing certain modifications in the web interface allowing an authenticated attacker to influence the user interface configured by an administrator.
- CVE-2023-2650: (Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow
- CVE-2023-44318: (Use of Hard-coded Cryptographic Key Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices use a hardcoded key to obfuscate the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative

privileges or an attacker that obtains a configuration backup to extract configuration information from the exported file

- CVE-2023-44317: (Insufficient Verification of Data Authenticity Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected products do not properly validate the content of uploaded X509 certificates which could allow an attacker with administrative privileges to execute arbitrary code on the device.
- CVE-2023-44322: (Unchecked Return Value Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices can be configured to send emails when certain events occur on the device. When presented with an invalid response from the SMTP server, the device triggers an error that disrupts email sending. An attacker with access to the network can use this to do disable notification of users when certain events occur.
- CVE-2023-0401: (NULL Pointer Dereference Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAn-dEnveloped data. In case the hash algorithm used for the signature is known to the OpenSSL library but the implementation of the hash algorithm is not available the digest initialization will fail. There is a missing check for the return value from the initialization function which later leads to invalid usage of the digest API most likely leading to a crash. The unavailability of an algorithm can be caused by using FIPS enabled configuration of providers or more commonly by not loading the legacy provider. PKCS7 data is processed by the SMIME library calls and also by the time stamp (TS) library calls
- CVE-2023-0217: (NULL Pointer Dereference Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack
- CVE-2023-44321: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices do not properly validate the length of inputs when performing certain configuration changes in the web interface allowing an authenticated attacker to cause a denial of service condition. The device needs to be restarted for the web interface to become available again.
- CVE-2023-44319: (Use of Weak Hash Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices use a weak checksum algorithm to protect the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that tricks a legitimate administrator to upload a modified configuration file to change the configuration of an affected device.

- CVE-2023-44373: (Injection Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell. Follow-up of CVE-2022-36323.
- CVE-2023-0216: (NULL Pointer Dereference Vulnerability in Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family)
    - An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack
- CVE-2023-5984: (Download of Code Without Integrity Check Vulnerability in Schneider PowerLogic ION8650 and PowerLogic ION8800)
    - A CWE-494 Download of Code Without Integrity Check vulnerability exists that could allow modified firmware to be uploaded when an authorized admin user begins a firmware update procedure.
- CVE-2023-5985: (Improper Neutralization of Input During Web Page Generation Vulnerability in Schneider PowerLogic ION8650 and PowerLogic ION8800)
    - A CWE-79 Improper Neutralization of Input During Web Page Generation vulnerability exists that could cause compromise of a user's browser when an attacker with admin privileges has modified system values.
- CVE-2023-20273: (Cisco IOS XE Web UI Privilege Escalation Vulnerability in Rockwell Stratix 5800 & 5200)
    - Rockwell Automation is aware of active exploitation of a previously unknown vulnerability in the Web UI feature of Cisco IOS XE Software when exposed to the internet or to untrusted networks. This vulnerability could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.

20231110

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

- **Talos Rules 2023-11-08 (https://www.snort.org/advisories/talos-rules-2023-11-08)**
- **Talos Rules 2023-11-07 (https://www.snort.org/advisories/talos-rules-2023-11-07)**

The new and updated Snort rules span the following categories:

- 3 malware-cnc rules with SIDs 62619, 62618, 62617
- 1 malware-other rules with SIDs 300749
- 1 os-windows rules with SIDs 62620

- 1 server-mail rules with SIDs 62622
- 2 server-webapp rules with SIDs 62623, 62621

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

- CVE-2023-4452: (Buffer Overflow Vulnerability in Moxa EDR-810/G902/G903 Series Web Server)
    - A vulnerability has been identified in the EDR-810, EDR-G902, and EDR-G903 Series, making them vulnerable to the denial-of-service vulnerability. This vulnerability stems from insufficient input validation in the URI, potentially enabling malicious users to trigger the device reboot.
- CVE-2023-5627: (Incorrect Implementation of Authentication Algorithm Vulnerability in Moxa NPort 6000 Series)
    - A vulnerability has been identified in NPort 6000 Series, making the authentication mechanism vulnerable. This vulnerability arises from the incorrect implementation of sensitive information protection, potentially allowing malicious users to gain unauthorized access to the web service.

20231103

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

- **Talos Rules 2023-11-02 (https://www.snort.org/advisories/talos-rules-2023-11-02)**
- **Talos Rules 2023-10-31 (https://www.snort.org/advisories/talos-rules-2023-10-31)**

The new and updated Snort rules span the following categories:

- 5 browser-chrome rules with SIDs 300745, 300741, 300746, 300744, 300743
- 1 browser-other rules with SIDs 300747
- 1 file-other rules with SIDs 300742
- 1 indicator-obfuscation rules with SIDs 29519
- 2 malware-cnc rules with SIDs 62599, 62598
- 1 os-mobile rules with SIDs 62606
- 3 os-windows rules with SIDs 300748, 62600, 62596
- 1 server-other rules with SIDs 62577
- 5 server-webapp rules with SIDs 62597, 62580, 62583, 62581, 62582