Release Notes for Cisco Cyber Vision Knowledge DB

Release 202304

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-4.2.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.2.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.2.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.2.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.2.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.2.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.2.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.2.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.2.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.2.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.2.0
Updates/KDB/KDB.202304	**Description**
CiscoCyberVision_knowledgedb_20230407.db	Knowledge DB version 20230407
CiscoCyberVision_knowledgedb_20230414.db	Knowledge DB version 20230414
CiscoCyberVision_knowledgedb_20230421.db	Knowledge DB version 20230421
CiscoCyberVision_knowledgedb_20230428.db	Knowledge DB version 20230428

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

20230428

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

- **Talos Rules 2023-04-27 (https://www.snort.org/advisories/talos-rules-2023-04-27)**
- **Talos Rules 2023-04-25 (https://www.snort.org/advisories/talos-rules-2023-04-25)**

The new and updated Snort rules span the following categories:

- 9 malware-cnc rules with SIDs 61664, 61665, 61676, 61679, 61680, 61681, 61682, 61683, 61684
- 8 malware-other rules with SIDs 300511, 300512, 300513, 300514, 300516, 300517, 300518, 300519
- 3 server-webapp rules with SIDs 60164, 61677, 61678
- 3 server-other rules with SIDs 25276, 61685, 61686
- 1 browser-chrome rule with SID 300520
- 1 file-identify rule with SID 300515
- 1 os-mobile rule with SID 300510
- 1 protocol-ftp rule with SID 42862

20230421

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

- **Talos Rules 2023-04-20 (https://www.snort.org/advisories/talos-rules-2023-04-20)**
- **Talos Rules 2023-04-18 (https://www.snort.org/advisories/talos-rules-2023-04-18)**

The new and updated Snort rules span the following categories:

- 1 malware-cnc rule with SID 61639
- 4 malware-other rules with SIDs 300505, 300506, 300507, 300508
- 5 server-webapp rules with SIDs 60581, 61629, 61630, 61631, 61632
- 1 malware-tools rule with SIDs 300504
- 4 os-other rules with SIDs 300225, 300501, 300502, 300503
- 1 malware-backdoor rule with SID 300509
- 1 file-other rule with SID 37650

20230414

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

- **Talos Rules 2023-04-13 (https://www.snort.org/advisories/talos-rules-2023-04-13)**
- **Talos Rules 2023-04-11 (https://www.snort.org/advisories/talos-rules-2023-04-11)**
- **Talos Rules 2023-04-10 (https://www.snort.org/advisories/talos-rules-2023-04-10)**

The new and updated Snort rules span the following categories:

- 2 malware-cnc rules with SIDs 61612, 61627
- 7 server-webapp rules with SIDs 60598, 300493, 300494, 61621, 61622, 61623, 61624
- 1 server-other rule with SIDs 25276
- 1 browser-chrome rule with SIDs 300497
- 8 os-windows rules with the SID 300496, 300498, 300499, 300500, 61613, 61614, 61619, 61620
- 1 os-mobile rule with the SID 300277
- 1 file-other rule with the SID 300495

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

- CVE-2020-28895: (Integer Overflow Vulnerability in Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families)
  - In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
- CVE-2020-35198: (Integer Overflow Vulnerability in Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families)
  - An issue was discovered in Wind River VxWorks. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
- CVE-2022-1652: (Use After Free Vulnerability in Siemens SCALANCE XCM332)
  - Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.
- CVE-2022-35252: (Improper Validation Vulnerability in Siemens SCALANCE XCM332)
  - When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.

- CVE-2022-30065: (Race Condition Vulnerability in Siemens SCALANCE XCM332)
    - A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.
- CVE-2022-1729: (Race Condition Vulnerability in Siemens SCALANCE XCM332)
    - A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.
- CVE-2022-32205: (Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SCALANCE XCM332)
    - A malicious server can serve excessive amounts of "Set-Cookie:" headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error. This denial state might remain for as long as the same cookies are kept, match and haven't expired. Due to cookie matching rules, a server on "foo.example.com" can set cookies that also would match for "bar.example.com", making it it possible for a "sister server" to effectively cause a denial of service for a sibling site on the same second level domain using this method.
- CVE-2022-32206: (Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SCALANCE XCM332)
    - curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors.
- CVE-2022-32207: (Incorrect Default Permissions Vulnerability in Siemens SCALANCE XCM332)
    - When curl < 7.84.0 saves cookies, alt-svc and hsts data to local files, it makes the operation atomic by finalizing the operation with a rename from a temporary name to the final target file name.In that rename operation, it might accidentally widen the permissions for the target file, leaving the updated file accessible to more users than intended.
- CVE-2022-32208: (Out-of-bounds Write Vulnerability in Siemens SCALANCE XCM332)
    - When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.
- CVE-2022-40674: (Use After Free Vulnerability in Siemens SCALANCE XCM332)
    - libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.
- CVE-2023-28489: (Command Injection Vulnerability in CPCI85 Firmware of Siemens SICAM A8000 Devices)

  - The CPCI85 firmware of SICAM A8000 CP-8031 and CP-8050 is affected by unauthenticated command injection vulnerability. This could allow an attacker to perfom remote code execution.

- CVE-2023-29054: (Weak Encryption Vulnerability in Siemens SCALANCE X-200IRT Devices)
  - The SSH server on affected devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.
- CVE-2023-25619: (Improper Check for Unusual or Exceptional Conditions Vulnerability in Schneider Modicon PLCs and PACs)
  - Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when communicating over the Modbus TCP protocol.
- CVE-2023-25620: (Improper Check for Unusual or Exceptional Conditions Vulnerability in Schneider Modicon PLCs and PACs)
  - Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause denial of service of the controller when a malicious project file is loaded onto the controller by an authenticated user.
- CVE-2021-46828: (Allocation of Resources Without Limits or Throttling Vulnerability in Siemens SCALANCE XCM332)
  - In libtirpc before 1.3.3rc1, remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in turn, lead to an svc_run infinite loop without accepting new connections.
- CVE-2023-28766: (Denial of Service Vulnerability in Siemens SIPROTEC 5 Devices)
  - Affected devices lack proper validation of http request parameters of the hosted web service. An unauthenticated remote attacker could send specially crafted packets that could cause denial of service condition of the target device.
- CVE-2023-1109: (Directory Traversal Vulnerability in Phoenix Contact ENERGY AXC PU and SMARTRTU AXC)
  - An authenticated restricted user of the web frontend can access, read, write and create files throughout the file system using specially crafted URLs via the upload and download functionality of the web service.

20230407

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

- **Talos Rules 2023-04-06 (https://www.snort.org/advisories/talos-rules-2023-04-06)**
- **Talos Rules 2023-04-04 (https://www.snort.org/advisories/talos-rules-2023-04-04)**

The new and updated Snort rules span the following categories:

- 2 protocol-voip rule with SIDs 61577, 61578

- 10 malware-other rules with SIDs 300483, 300484, 300485, 300486, 300487, 300488, 300489, 300490, 300491, 300492
- 5 malware-cnc rules with SIDs 61564, 61565, 61566, 61567, 61588
- 3 server-webapp rules with SIDs 61579, 61580, 61581
- 1 os-windows rule with the SID 300482
- 1 os-mobile rule with the SID 61576