Release Notes for Cisco Cyber Vision Knowledge DB

Release 202303

Compatible device list ***2***

Links ***2***

Software Download **2**

Related Documentation **3**

Database download ***3***

How to update the database ***3***

Release contents ***4***

20230331 .... **4**

20230324 .... **4**

20230317 .... **5**

20230310 .... **14**

20230303 .... **15**

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.202303	**Description**
CiscoCyberVision_knowledgedb_20230303.db	Knowledge DB version 20230303
CiscoCyberVision_knowledgedb_20230310.db	Knowledge DB version 20230310
CiscoCyberVision_knowledgedb_20230317.db	Knowledge DB version 20230317
CiscoCyberVision_knowledgedb_20230324.db	Knowledge DB version 20230324
CiscoCyberVision_knowledgedb_20230331.db	Knowledge DB version 20230331

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

20230331

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

- **Talos Rules 2023-03-30 (https://www.snort.org/advisories/talos-rules-2023-03-30-3-30-2023)**
- **Talos Rules 2023-03-30 (https://www.snort.org/advisories/talos-rules-2023-03-30)**
- **Talos Rules 2023-03-28 (https://www.snort.org/advisories/talos-rules-2023-03-28)**

The new and updated Snort rules span the following categories:

- 1 policy-other rule with SID 61514
- 2 malware-backdoor rules with SIDs 300480, 300481
- 7 malware-other rules with SIDs 61539, 300470, 300471, 300472, 300474, 300475, 300476
- 7 malware-cnc rules with SIDs 61507, 61508, 61509, 61510, 61511, 61512, 61513
- 8 server-other rule with SID 61291, 61358, 61516, 61525, 61546, 61547, 61548, 61549
- 11 server-webapp rules with SIDs 39908, 61515, 61531, 61534, 61537, 61538, 61540, 61541, 300477, 300478, 300479
- 1 os-windows rule with the SID 61526
- 1 file-identify rule with the SID 300476
- 1 file-other rule with the SID 49864

20230324

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

- **Talos Rules 2023-03-23 (https://www.snort.org/advisories/talos-rules-2023-03-23)**
- **Talos Rules 2023-03-21 (https://www.snort.org/advisories/talos-rules-2023-03-21)**

The new and updated Snort rules span the following categories:

- 1 policy-other rule with SID 61498
- 5 malware-other rules with SIDs 61490, 61495, 300465, 300467, 300468
- 3 malware-cnc rules with SIDs 61489, 61493, 61494
- 1 file-office rule with SID 300469
- 17 server-webapp rules with SIDs 60670, 60671, 60672, 60673, 60674, 60675, 60676, 60677, 60678, 61483, 61484, 61485, 61486, 61499, 61500, 61501, 61502
- 1 os-windows rule with the SID 300466

20230317

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

- **Talos Rules 2023-03-15 (https://www.snort.org/advisories/talos-rules-2023-03-15)**
  - Talos is releasing coverage for a Microsoft Outlook Escalation of Privilege vulnerability, CVE-2023-23397. The Snort 2 SIDs for this are 61478-61479, the Snort 3 SID for this is 300464.
  - Talos also has added and modified multiple rules in the file-image, file-office, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-03-14 (https://www.snort.org/advisories/talos-rules-2023-03-14)**
  - Microsoft Vulnerability CVE-2023-23410: A coding deficiency exists in Microsoft Windows HTTP.sys that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 61464 through 61465, Snort 3: GID 1, SID 300460.
  - Microsoft Vulnerability CVE-2023-23416: A coding deficiency exists in Windows Cryptographic Services that may lead to remote code execution.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 61466 through 61467, Snort 3: GID 1, SID 300461.
  - Talos also has added and modified multiple rules in the deleted, malware-other, os-windows, policy-other, protocol-scada 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-2021-4034: (Out-of-bounds Write Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine
- CVE-2022-32206: (Allocation of Resources Without Limits or Throttling Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - curl < 7.84.0 supports “chained” HTTP compression algorithms, meaning that a server response 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 to and returning out of memory errors.

- CVE-2022-30065: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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-2021-42379: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the next_input_file function.
- CVE-2021-26401: (Improper Locking Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - LFENCE/JMP (mitigation V2-2) may not sufficiently mitigate CVE-2017-5715 on some AMD CPUs.
- CVE-2021-42386: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the nvalloc function.
- CVE-2022-1652: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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-2022-1975: (Uncaught Exception Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - There is a sleep-in-atomic bug in /net/nfc/netlink.c that allows an attacker to crash the Linux kernel by simulating a nfc device from user-space.
- CVE-2022-35252: (Buffer Overflow Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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 HTTPserver might make the server return 400 responses. Effectively allowing a"sister site" to deny service to all siblings.
- CVE-2022-28356: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c.
- CVE-2022-1729: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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-2022-0002: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)

    - Non-transparent sharing of branch predictor within a context in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access

- CVE-2022-0001: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - Non-transparent sharing of branch predictor selectors between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.
- CVE-2022-1292: (OS Command Injection Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - The c_rehash script does not properly sanitise shell metacharacters to prevent command injection.
- CVE-2022-1353: (Improper Certificate Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A vulnerability was found in the pfkey_register function in net/key/af_key.c in the Linux kernel. This flaw allows a local, unprivileged user to gain access to kernel memory, leading to a system crash or a leak of internal kernel information.
- CVE-2022-1516: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A NULL pointer dereference flaw was found in the Linux kernel's X.25 set of standardized network protocols functionality in the way a user terminates their session using a simulated Ethernet card and continued usage of this connection. This flaw allows a local user to crash the system.
- CVE-2021-42380: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the clrvar function
- CVE-2022-23041: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends
- CVE-2021-42373: (NULL Pointer Dereference Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A NULL pointer dereference in Busybox's man applet leads to denial of service when a section name is supplied but no page argument is given.
- CVE-2022-2588: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code

- CVE-2022-32207: (Incorrect Default Permissions Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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-2022-1734: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A flaw in Linux Kernel found in nfcmrvl_nci_unregister_dev() in drivers/nfc/nfcmrvl/main.c can lead to use after free both read or write when non synchronized between cleanup routine and firmware download routine.
- CVE-2021-42375: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - An incorrect handling of a special element in Busybox's ash applet leads to denial of service when processing a crafted shell command, due to the shell mistaking specific characters for reserved characters. This may be used for DoS under rare conditions of filtered command input.
- CVE-2022-23308: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.
- CVE-2022-32981: (Buffer Overflow Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - An issue was discovered in the Linux kernel through 5.18.3 on powerpc 32-bit platforms. There is a buffer overflow in ptrace PEEKUSER and POKEUSER (aka PEEKUSR and POKEUSR) when accessing floating point registers.
- CVE-2021-4149: (Improper Locking Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock operation in btrfs. In this flaw, a user with a local privilege may cause a denial of service (DOS) due to a deadlock problem.
- CVE-2022-0494: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw allows a local attacker with a special user privilege (CAP_SYS_ADMIN or CAP_SYS_RAWIO) to create issues with confidentiality.
- CVE-2022-32296: (Observable Discrepancy Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. This occurs because of use of Algorithm 4 ("Double-Hash Port Selection Algorithm") of RFC 6056.

- CVE-2022-20158: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - In bdi_put and bdi_unregister of backing-dev.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed.
- CVE-2022-26490: (Buffer Overflow Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters
- CVE-2022-32208: (Incorrect Default Permissions Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - 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-2022-1343: (Improper Certificate Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - Under certain circumstances, the command line OCSP verify function reports successful verification when the varification in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result.
- CVE-2022-28390: (Double Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free.
- CVE-2022-1198: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A use-after-free vulnerabilitity was discovered in drivers/net/hamradio/6pack.c of linux that allows an attacker to crash linux kernel by simulating ax25 device using 6pack driver from user space.
- CVE-2022-30594: (Incorrect Authorization Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.
- CVE-2022-36879: (Buffer Overflow Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice
- CVE-2022-23040: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends

- CVE-2019-1125: (Exposure of Sensitive Information Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'
- CVE-2022-1473: (Improper Certificate Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - The used OpenSSL version improperly reuses memory when decoding certificates or keys. This can lead to a process termination and Denial of Service for long lived processes.
- CVE-2022-1199: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A flaw was found in the Linux kernel. This flaw allows an attacker to crash the Linux kernel by simulating amateur radio from the user space, resulting in a null-ptr-deref vulnerability and a use-after-free vulnerability.
- CVE-2022-23042: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends
- CVE-2022-0547: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials.
- CVE-2022-1011: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - A use-after-free flaw was found in the Linux kernel's FUSE filesystem in the way a user triggers write().This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, resulting in privilege escalation.
- CVE-2022-2380: (Out-of-bounds Write Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - The Linux kernel was found vulnerable out of bounds memory access in the drivers/video/fbdev/sm712fb.c:smtcfb_read() function. The vulnerability could result in local attackers being able to crash the kernel.
- CVE-2022-36946: (Improper Input Validation Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
  - nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.

- CVE-2022-23038: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends
- CVE-2022-1304: (Out-of-bounds Write Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.
- CVE-2022-2639: (Integer Underflow Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - An integer coercion error was found in the openvswitch kernel module. Given a sufficiently large number of actions, while copying and reserving memory for a new action of a new flow, the reserve_sfa_size() function does not return -EMSGSIZE as expected, potentially leading to an out-of-bounds write access. This flaw allows a local user to crash or potentially escalate their privileges on the system.
- CVE-2022-1016: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A flaw was found in the Linux kernel in net/netfilter/nf_tables_core.c:nft_do_chain, which can cause a use-after-free. This issue needs to handle 'return' with proper preconditions, as it can lead to a kernel information leak problem caused by a local, unprivileged attacker.
- CVE-2022-1974: (Use After Free Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - A use-after-free flaw was found in the Linux kernel's NFC core functionality due to a race condition between kobject creation and delete. This vulnerability allows a local attacker with CAP_NET_ADMIN privilege to leak kernel information.
- CVE-2022-23039: (Race Condition Vulnerability in Multiple Siemens RUGGEDCOM and SCALANCE Products)
    - Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends
- CVE-2018-25032: (Out-of-bounds Write Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.
- CVE-2021-42382: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_s function.
- CVE-2018-12886: (Sensitive Information Disclosure Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)

    - stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.
- CVE-2021-42384: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the handle_special function.
- CVE-2021-42385: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.
- CVE-2021-42377: (Release of Invalid Pointer or Reference Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - An attacker-controlled pointer free in Busybox's hush applet leads to denial of service and possible code execution when processing a crafted shell command, due to the shell mishandling the &&& string. This may be used for remote code execution under rare conditions of filtered command input.
- CVE-2021-42381: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the hash_init function.
- CVE-2021-42378: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_i function.
- CVE-2021-42376: (NULL Pointer Dereference Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell command, due to missing validation after a \x03 delimiter character. This may be used for DoS under very rare conditions of filtered command input.
- CVE-2021-42383: (Use After Free Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.
- CVE-2022-23395: (Prototype Pollution Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)
    - jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS).
- CVE-2021-42374: (Out-of-bounds Read Vulnerability in Siemens SCALANCE W-700 IEEE 802.11ax devices)

  - An out-of-bounds heap read in Busybox’s unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that internally supports LZMA compression.
- CVE-2022-38767: (Denial of Service Vulnerability in the RADIUS Client of Siemens SIPROTEC 5 Devices)
  - An issue was discovered in Wind River VxWorks 6.9 and 7, that allows a specifically crafted packet sent by a Radius server, may cause Denial of Service during the IP Radius access procedure.
- CVE-2023-0215: (Use After Free Vulnerability in Siemens SCALANCE W1750D Devices)
  - The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. In some cases, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to a previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash.
- CVE-2023-0286: (Improper Input Validation Vulnerability in Siemens SCALANCE W1750D Devices)
  - There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service.
- CVE-2022-4304: (Inadequate Encryption Strength Vulnerability in Siemens SCALANCE W1750D Devices)
  - 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-2022-4450: (Double Free Vulnerability in Siemens SCALANCE W1750D Devices)
  - 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.

- CVE-2023-1257: (Improper Physical Access Control in Moxa UC Series)
  - An attacker with physical access to the device can restart the device and gain access to its BIOS. Then, command line options can be altered, allowing the attacker to access the terminal. From the terminal, the attacker can modify the device authentication files to create a new user profile and gain full access to the system.
- CVE-2022-43994: (Improper Certificate Validation in Moxa NPort 6000 Series)
  - There is no client certificate verification/authentication performed on the secure connection. An attacker may perform a person-in-the-middle attack and eavesdrop on the secure connection between the NPort 6000 Series and the Windows driver manager.
- CVE-2022-43993: (Improper Certificate Validation in Moxa NPort 6000 Series)
  - The Windows driver manager software does not perform any certificate verification. An attacker may execute a person-in-the-middle attack and eavesdrop on the secure connection between the NPort 6000 Series and the Windows driver manager.
- CVE-2023-20064: (Cisco IOS XR Software Bootloader Unauthenticated Information Disclosure Vulnerability)
  - A vulnerability in the GRand Unified Bootloader (GRUB) for Cisco IOS XR Software could allow an unauthenticated attacker with physical access to the device to view sensitive files on the console using the GRUB bootloader command line. This vulnerability is due to the inclusion of unnecessary commands within the GRUB environment that allow sensitive files to be viewed. An attacker could exploit this vulnerability by being connected to the console port of the Cisco IOS XR device when the device is power-cycled. A successful exploit could allow the attacker to view sensitive files that could be used to conduct additional attacks against the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.
- CVE-2023-20049: (Cisco IOS XR Software for ASR 9000 Series Routers Bidirectional Forwarding Detection Denial of Service Vulnerability)
  - A vulnerability in the bidirectional forwarding detection (BFD) hardware offload feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers, ASR 9902 Compact High-Performance Routers, and ASR 9903 Compact High-Performance Routers could allow an unauthenticated, remote attacker to cause a line card to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of malformed BFD packets that are received on line cards where the BFD hardware offload feature is enabled. An attacker could exploit this vulnerability by sending a crafted IPv4 BFD packet to an affected device. A successful exploit could allow the attacker to cause line card exceptions or a hard reset, resulting in loss of traffic over that line card while the line card reloads.

20230310

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

- **Talos Rules 2023-03-09 (https://www.snort.org/advisories/talos-rules-2023-03-09)**
    - Talos has added and modified multiple rules in the file-office, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-03-07 (https://www.snort.org/advisories/talos-rules-2023-03-07)**
    - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20230303

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

- **Talos Rules 2023-03-02 (https://www.snort.org/advisories/talos-rules-2023-03-02**)
    - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2023-02-28 (https://www.snort.org/advisories/talos-rules-2023-02-28)**
    - Talos has added and modified multiple rules in the malware-cnc, malware-other, os-windows, policy-other, protocol-scada 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-2023-20050: (Cisco NX-OS Software CLI Command Injection Vulnerability)
    - A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the currently logged-in user.