Release Notes for Cisco Cyber Vision Knowledge DB

Release 202411

Compatible device list

Center	Description
All version 4 and 5 centers	All Cisco Cyber Vision center version 4 and 5 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-5.0.1.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.0.1.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.0.1.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.0.1.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-5.0.1.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.0.1.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.0.1.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.0.1.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-5.0.1.dat	Knowledge DB embedded in Cisco Cyber Vision 5.0.1
Updates/KDB/KDB.202411	**Description**
CiscoCyberVision_knowledgedb_20241108.db	Knowledge DB version 20241108
CiscoCyberVision_knowledgedb_20241115.db	Knowledge DB version 20241115

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

20241115

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

- **Talos Rules 2024-11-14 (https://www.snort.org/advisories/talos-rules-2024-11-14)**
- **Talos Rules 2024-11-12 (https://www.snort.org/advisories/talos-rules-2024-11-12)**

The new and updated Snort rules span the following categories:

- 1 browser-firefox rule with SID 301074
- 3 malware-cnc rules with SIDs 64235, 301057, 64217
- 9 malware-other rules with SIDs 301070, 301061, 301059, 301069, 301058, 301062, 301060, 301072, 301063
- 2 os-other rules with SIDs 64088, 64087
- 8 os-windows rules with SIDs 301065, 300612, 301073, 301066, 64218, 301064, 64229, 64234
- 1 protocol-scada rule with SID 24425
- 1 protocol-tftp rule with SID 519
- 5 server-other rules with SIDs 9790, 44683, 58239, 58240, 58241
- 11 server-webapp rules with SIDs 18793, 301068, 18792, 301067, 64240, 301075, 41026, 29549, 64242, 301071, 64241

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

- CVE-2024-41798: (Improper Authentication Vulnerability in Siemens SENTRON PAC3200)
  - Affected devices only provide a 4-digit PIN to protect from administrative access via Modbus TCP interface. Attackers with access to the Modbus TCP interface could easily bypass this protection by brute-force attacks or by sniffing the Modbus clear text communication.
- CVE-2024-46887: (Unauthenticated Information Disclosure in Web Server of Siemens SIMATIC S7-1500 CPUs)
  - The web server of affected devices do not properly authenticate user request to the '/ClientArea/Run-timeInfoData.mwsl' endpoint. This could allow an unauthenticated remote attacker to gain knowledge about current actual and configured maximum cycle times as well as about configured maximum communication load.
- CVE-2022-28613: (Improper Input Validation Vulnerability in Hitachi Energy RTU500 series)
  - Successful exploitation of this vulnerability could cause an internal buffer overflow, which can reboot the product. A vulnerability exists in the HCI Modbus TCP function included in the affected product versions. If the HCI Modbus TCP is enabled and configured, then an attacker could exploit

the vulnerability by sending a specially crafted message to the RTU500, causing the receiving RTU500 CMU to reboot. The vulnerability is caused by a validation error in the length information carried in MBAP header in the HCI Modbus TCP function.CVE-2022-28613 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

- CVE-2022-2081: (Stack-based Buffer Overflow Vulnerability in Hitachi Energy RTU500)
    - Successful exploitation of this vulnerability could allow an attacker to send a specially crafted Modbus TCP packet in a high rate, causing a stack overflow, which could result in a reboot of the product. This vulnerability exists in the HCI Modbus TCP function in affected product versions. If the HCI Modbus TCP is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500 in a high rate, causing the targeted RTU500 CMU to reboot. There is a lack of flood control, which if exploited, could cause an internal stack overflow in the HCI Modbus TCP function.CVE-2022-2081 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
- CVE-2024-1531: (Unrestricted Upload of File with Dangerous Type Vulnerability in Hitachi Energy RTU500 Series)
    - Successful exploitation of these vulnerabilities could allow the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. A vulnerability exists in the stb-language file handling that affects the RTU500 series product versions listed below. A malicious actor could print random memory content in the RTU500 system log, if an authorized user uploads a specially crafted stb-language file.
- CVE-2024-1532: (Unrestricted Upload of File with Dangerous Type Vulnerability in Hitachi Energy RTU500 Series)
    - Successful exploitation of these vulnerabilities could allow the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. A vulnerability exists in the stb-language file handling that affects the RTU500 series product versions listed below. A malicious actor could enforce diagnostic texts being displayed as empty strings, if an authorized user uploads a specially crafted stb-language file.
- CVE-2022-3353: (Improper Resource Shutdown or Release Vulnerability in Hitachi Energy IEC 61850 MMS-Server)
    - Successful exploitation of this vulnerability could cause products using the IEC 61850 MMS-server communication stack to stop accepting new MMS-client connections. An attacker could exploit the IEC 61850 MMS-Server communication stack by forcing the communication stack to stop accepting new MMS-client connections. CVE-2022-3353 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been assigned; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
- CVE-2022-2502: (Stack-based Buffer Overflow Vulnerability in Hitachi Energy RTU500 series)

  - Successful exploitation of these vulnerabilities could cause a buffer overflow and reboot of the product. A vulnerability exists in the HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited if the HCI 60870-5-104 is configured with IEC 62351-5 support and the CMU contains the license feature 'Advanced security' which must be ordered separately. If these preconditions are fulfilled, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a missing input data validation, which eventually, if exploited, could cause an internal buffer to overflow in the HCI IEC 60870-5-104 function.

- CVE-2022-4608: (Stack-based Buffer Overflow Vulnerability in Hitachi Energy RTU500 series)
  - Successful exploitation of these vulnerabilities could cause a buffer overflow and reboot of the product. A vulnerability exists in HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited if the HCI 60870-5-104 is configured with support for IEC 62351-3. After session resumption interval is expired, an RTU500 initiated update of session parameters could cause an unexpected restart due to a stack overflow.
- CVE-2023-0286: (Access of Resource Using Incompatible Type ('Type Confusion') Vulnerability in Hitachi Energy's RTU500 Series Product)
  - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. There is a type-confusion vulnerability affecting X.400 address processing within an X.509 GeneralName. This vulnerability could allow an attacker to pass arbitrary pointers to a memcmp call, enabling access to read memory contents or cause a denial-of-service condition.X.400 addresses parsed as an ASN1_STRING while the public structure definition for GENERAL_NAME incorrectly specifies the x400Address field type as ASN1_TYPE.
- CVE-2022-4304: (Observable Timing Discrepancy Vulnerability in Hitachi Energy's RTU500 Series Product)
  - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. A timing-based side channel exists in the OpenSSL RSA Decryption implementation. This could allow an attacker sufficient access to recover plaintext across a network to perform a Bleichenbacher style attack. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE.
- CVE-2022-23937: (Out-of-bounds Read Vulnerability in Hitachi Energy's RTU500 Series Product)
  - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. A vulnerability exists in the Wind River VxWorks version 6.9 affecting the RTU500 series product versions listed. An attacker could exploit the vulnerability by using a specific crafted packet that could lead to an out-of-bounds read during an IKE initial exchange scenario.
- CVE-2022-0778: (Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability in Hitachi Energy's RTU500 Series Product)
  - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. A vulnerability exists in the OpenSSL version 1.0.2 that affects the RTU500 Series product versions listed. An attacker can exploit the BN_mod_sqrt()

function to compute a modular square root that contains a bug causing a continual loop for non-prime moduli.

- CVE-2021-3711: (Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') Vulnerability in Hitachi Energy's RTU500 Series Product)
    - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. A vulnerability exists in the OpenSSL Version 1.0.2 affecting the RTU500 Series product versions listed. An attacker with access to applications and the capability to present SM2 content for decryption could cause a buffer overflow up to a maximum of 62 bytes while altering contents of data present after the buffer. This vulnerability could allow an attacker to change application behavior or cause the application to crash.
- CVE-2021-3712: (Out-of-bounds Read Vulnerability in Hitachi Energy's RTU500 Series Product)
    - Successful exploitation of these vulnerabilities could allow an attacker to crash the device being accessed or cause a denial-of-service condition. A vulnerability exists in the OpenSSL Version 1.0.2 affecting the RTU500 Series product versions listed. A malicious actor could cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions. Exploiting this vulnerability could create a system crash causing a denial-of-service condition or a disclosure of private memory contents, such as private keys or sensitive plaintext.
- CVE-2023-6711: (Improper Input Validation in DoS Vulnerability in Hitachi Energy’s RTU500 series products)
    - Hitachi Energy is aware of DoS vulnerability that affects the RTU500 series product versions listed in this document. If the vulnerability is exploited, it could affect the availability of the device. Please refer to the Recommended Immediate Actions for information about the mitigation/remediation.
- CVE-2023-5767: (Cross-site scripting Vulnerability in Hitachi Energy’s RTU500 series Product)
    - Hitachi Energy is aware of the vulnerabilities CVE-2023-5767, CVE-2023-5768 and CVE-2023-5769 in the Web server and HCI IEC 60870-5-104 component, that affects the RTU500 versions that are listed below. An attacker successfully exploiting these vulnerabilities could perform cross-site scripting on web server or denial of service on HCI IEC 60870-5-104. Please refer to the Recommended Immediate Actions for information about the available mitigation/remediation strategies.
- CVE-2023-5768: (Cross-site scripting Vulnerability in Hitachi Energy’s RTU500 series Product)
    - Hitachi Energy is aware of the vulnerabilities CVE-2023-5767, CVE-2023-5768 and CVE-2023-5769 in the Web server and HCI IEC 60870-5-104 component, that affects the RTU500 versions that are listed below. An attacker successfully exploiting these vulnerabilities could perform cross-site scripting on web server or denial of service on HCI IEC 60870-5-104. Please refer to the Recommended Immediate Actions for information about the available mitigation/remediation strategies.
- CVE-2023-5769: (Cross-site scripting Vulnerability in Hitachi Energy’s RTU500 series Product)
    - Hitachi Energy is aware of the vulnerabilities CVE-2023-5767, CVE-2023-5768 and CVE-2023-5769 in the Web server and HCI IEC 60870-5-104 component, that affects the RTU500 versions that are

listed below. An attacker successfully exploiting these vulnerabilities could perform cross-site scripting on web server or denial of service on HCI IEC 60870-5-104. Please refer to the Recommended Immediate Actions for information about the available mitigation/remediation strategies.

- CVE-2023-1514: (Improper Certificate Validation Vulnerability in Hitachi Energy's RTU500 series Product)
    - Hitachi Energy is aware of a reported vulnerability in the RTU500 Scripting interface. When a client connects to a server using TLS, the server presents a certificate. This certificate links a public key to the identity of the service and is signed by a Certification Authority (CA), allowing the client to validate that the remote service can be trusted and is not malicious. If the client does not validate the parameters of the certificate, then attackers could be able to spoof the identity of the service.
- CVE-2020-1968: (Observable Discrepancy Vulnerability in Hitachi Energy RTU500 series)
    - Successful exploitation of these vulnerabilities could allow an attacker to eavesdrop on traffic, retrieve information from memory, or cause a denial-of-service condition. The Raccoon attack exploits a flaw in the TLS specification, which can lead to an attacker computing pre-master secret in connections that have used a Diffie-Hellman- based cipher suite. An attacker can then eavesdrop on all encrypted communications sent over the exploited TLS connection.CVE-2020-1968 has been assigned to this vulnerability. A CVSS v3 base score of 3.7 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
- CVE-2020-24977: (Buffer Over-read Vulnerability in Hitachi Energy RTU500 series)
    - Successful exploitation of these vulnerabilities could allow an attacker to eavesdrop on traffic, retrieve information from memory, or cause a denial-of-service condition. There is a global buffer over-read vulnerability in xmlEncodeEntitiesInternal in the affected libxml2/entities.c.CVE-2020-24977 has been assigned to this vulnerability. A CVSS v3 base score of 6.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).
- CVE-2021-3517: (Out-of-bounds Read Vulnerability in Hitachi Energy RTU500 series)
    - Successful exploitation of these vulnerabilities could allow an attacker to eavesdrop on traffic, retrieve information from memory, or cause a denial-of-service condition. A vulnerability exists in the xml entity encoding functionality of the affected libxml2. An attacker can use a specially crafted file to trigger an out-of-bounds read.CVE-2021-3517 has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H).
- CVE-2021-35533: (Improper Input Validation Vulnerability in Hitachi Energy RTU500 series BCI)
    - Successful exploitation of this vulnerability could allow a remote attacker to reboot the device. An issue exists in the BCI IEC 60870-5-104 function included in the affected products. If BCI IEC 60870-5-104 is enabled and configured, an attacker could exploit the vulnerability by sending a specially crafted message to the affected product, causing it to reboot. This vulnerability is caused by the validation error in the APDU parser of the BCI IEC 60870-5-104 function.CVE-2021-35533 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

- CVE-2020-36229: (Access of Resource Using Incompatible Type ('Type Confusion') Vulnerability in Hitachi Energy RTU500 OpenLDAP)
    - Successful exploitation of these vulnerabilities could cause a denial-of-service condition in the affected version of the RTU500 series product. A vulnerability exists in the affected OpenLDAP versions leading to an LDAP service crash in the parsing of a keystring, resulting in a denial-of-service condition.CVE-2020-36229 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
- CVE-2020-36230: (Reachable Assertion Vulnerability in Hitachi Energy RTU500 OpenLDAP)
    - Successful exploitation of these vulnerabilities could cause a denial-of-service condition in the affected version of the RTU500 series product. A vulnerability exists in the affected OpenLDAP versions leading in an assertion failure in an LDAP service in the parsing of a file, resulting in a denial-of-service condition.CVE-2020-36230 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
- CVE-2021-3506: (Out-of-bounds Read Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.
- CVE-2023-28450: (Missing Encryption of Sensitive Data Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. An issue was discovered in Dnsmasq before 2.90. The default maximum EDNS.0 UDP packet size was set to 4096 but should be 1232 because of DNS Flag Day 2020.
- CVE-2023-49441: (Integer Overflow or Wraparound Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. dnsmasq 2.9 is vulnerable to Integer Overflow via forward_query.
- CVE-2024-2511: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Issue summary: Some non-de Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain

conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

- CVE-2024-4603: (Excessive Iteration Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA 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 functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.
- CVE-2024-4741: (Use After Free Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations
- CVE-2024-5594: (Improper Output Neutralization for Logs Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. control channel: refuse control channel messages with nonprintable characters in them. Security scope: a malicious openvpn peer can send garbage to openvpn log, or cause high CPU load
- CVE-2024-26306: (Observable Discrepancy Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. iPerf3 before 3.17, when used with OpenSSL before 3.2.0 as a server with RSA authentication, allows a

timing side channel in RSA decryption operations. This side channel could be sufficient for an attacker to recover credential plaintext. It requires the attacker to send a large number of messages for decryption, as described in "Everlasting ROBOT: the Marvin Attack" by Hubert Kario.

- CVE-2024-26925: (Improper Locking Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: release mutex after nft_gc_seq_end from abort path The commit mutex should not be released during the critical section between nft_gc_seq_begin() and nft_gc_seq_end(), otherwise, async GC worker could collect expired objects and get the released commit lock within the same GC sequence. nf_tables_module_autoload() temporarily releases the mutex to load module dependencies, then it goes back to replay the transaction again. Move it at the end of the abort phase after nft_gc_seq_end() is called.
- CVE-2024-28882: (Missing Release of Resource after Effective Lifetime Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. OpenVPN from 2.6.0 through 2.6.10 in a server role accepts multiple exit notifications from authenticated clients which will extend the validity of a closing session
- CVE-2024-50557: (Improper Input Validation Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Affected devices do not properly validate input in configuration fields of the iperf functionality. This could allow an unauthenticated remote attacker to execute arbitrary code on the device.
- CVE-2024-50558: (Improper Access Control Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Affected devices improperly manage access control for read-only users. This could allow an attacker to cause a temporary denial of service condition.
- CVE-2024-50559: (Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
    - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Affected devices do not properly validate the filenames of the certificate. This could allow an authenticated remote attacker to append arbitrary values which will lead to compromise of integrity of the system.
- CVE-2024-50560: (Improper Input Validation Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)

  - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Affected devices truncates usernames longer than 15 characters when accessed via SSH or Telnet. This could allow an attacker to compromise system integrity.

- CVE-2024-50561: (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
  - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. Affected devices do not properly sanitize the filenames before uploading. This could allow an authenticated remote attacker to compromise of integrity of the system.
- CVE-2024-50572: (Improper Neutralization of Special Elements in Siemens Output Used by a Downstream Component ('Injection') Vulnerability in Siemens SCALANCE M-800 Family Before V8.2)
  - SCALANCE M-800 family before V8.2 is affected by multiple vulnerabilities. Siemens has released new versions for the affected products and recommends to update to the latest versions. 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.
- CVE-2024-50310: (Incorrect Authorization Vulnerability in Siemens SIMATIC CP 1543-1 Devices)
  - SIMATIC CP 1543-1 devices contain an Incorrect Authorization vulnerability that could allow an unauthenticated attacker to gain access to the filesystem. Siemens has released a new version for SIMATIC CP 1543-1 V4.0 and recommends to update to the latest version. Affected devices do not properly handle authorization. This could allow an unauthenticated remote attacker to gain access to the filesystem.
- CVE-2024-8936: (Improper Input Validation Vulnerability in Schneider Electric Modicon Controllers M340 / Momentum / MC80)
  - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 products/ Modicon PAC control and monitor industrial operations. Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controller, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.
- CVE-2024-8937: (Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in Schneider Electric Modicon Controllers M340 / Momentum / MC80)
  - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 products/ Modicon PAC control and monitor industrial operations. Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controller, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.
- CVE-2024-8938: (Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in Schneider Electric Modicon Controllers M340 / Momentum / MC80)

- Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 products/ Modicon PAC control and monitor industrial operations. Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controller, which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller. CVE-2024-8933: (Improper Enforcement of Message Integrity During Transmission in a Communication Channel Vulnerability in Schneider Electric Modicon Controllers M340 / Momentum / MC80)
    - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controll which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.
- CVE-2024-8935: (Authentication Bypass by Spoofing Vulnerability in Schneider Electric Modicon Controllers M340 / Momentum / MC80)
    - Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M340 / Momentum / MC80 Failure to apply the provided remediations/mitigations below may risk unauthorized access to the controll which could result in the possibility of denial of service and loss of confidentiality, integrity of the controller.

20241108

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

- **Talos Rules 2024-11-07 (https://www.snort.org/advisories/talos-rules-2024-11-07)**
- **Talos Rules 2024-11-04 (https://www.snort.org/advisories/talos-rules-2024-11-04)**

The new and updated Snort rules span the following categories:

- 4 browser-plugins rules with SIDs 29538, 17588, 21560, 21558
- 2 malware-cnc rules with SIDs 301055, 60517
- 3 malware-other rules with SIDs 64189, 301054, 301056
- 1 protocol-pop rule with SID 1866
- 1 server-oracle rule with SID 59865
- 2 server-other rules with SIDs 16514, 64194
- 15 server-webapp rules with SIDs 60608, 64199, 64200, 64192, 54012, 25534, 64191, 64190, 61370, 61371, 64198, 64193, 64195, 64202, 64201