Release Notes for Cisco Cyber Vision Knowledge DB

Release 202201

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.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/4/4	**Description**
CiscoCyberVision-Embedded-KDB-4.dat	Knowledge DB embedded in Cisco Cyber Vision 4
Updates/KDB/KDB.202201	**Description**
CiscoCyberVision_knowledgedb_20220107.db	Knowledge DB version 20220107
CiscoCyberVision_knowledgedb_20220114.db	Knowledge DB version 20220114
CiscoCyberVision_knowledgedb_20220121.db	Knowledge DB version 20220121
CiscoCyberVision_knowledgedb_20220128.db	Knowledge DB version 20220128

Related Documentation

- Cisco Cyber Vision GUI User Guide:

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_GUI_User_Guide_4_0_0.pdf

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

20220128

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

- **Talos Rules 2022-01-27 (https://www.snort.org/advisories/talos-rules-2022-01-27)**
  - Talos has created the following rules, SIDs 58955-58956, to address CVE-2021-4034, a local privilege escalation vulnerability in Polkit's pkexec utility.
  - Talos has added and modified multiple rules in the browser-ie, file-executable, file-image, file-other, malware-cnc, malware-other, os-linux and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-01-25 (https://www.snort.org/advisories/talos-rules-2022-01-25)**
  - Talos has added and modified multiple rules in the malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-01-20 (https://www.snort.org/advisories/talos-rules-2022-01-20)**
  - Talos has added and modified multiple rules in the file-other and protocol-scada rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-01-18 (https://www.snort.org/advisories/talos-rules-2022-01-18)**
  - Talos has added and modified multiple rules in the file-other, file-pdf, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-22509: (Incorrect Privilege Assignment in FL SWITCH 2xxx series)
  An unprivileged user connected via SSH Command Line Interface (CLI) gains admin privileges. The user management of the FL SWITCH 2xxx family of devices implements access rights based on roles and permission groups. An unprivileged user logged in via the SSH CLI is assigned to the admin role independent of his configured access role enabling full access to the device configuration (CWE-266 - Incorrect Privilege Assignment). An attacker could elevate his privileges and take over control of the device.

20220121

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

- CVE-2022-20655: (Multiple Cisco Products CLI Command Injection Vulnerability)
  A vulnerability in the implementation of the CLI for multiple Cisco products could allow an authenticated, local attacker to perform a command injection attack. This vulnerability is due to insufficient validation of a process argument on an affected product. An attacker could exploit this vulnerability by injecting commands during the execution of this process. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of the management framework process, which are commonly root privileges.

20220114

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

- **Talos Rules 2022-01-13 (https://www.snort.org/advisories/talos-rules-2022-01-13)**
  - Talos has added and modified multiple rules in the malware-cnc, server-mysql and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-01-11 (https://www.snort.org/advisories/talos-rules-2022-01-11)**
  - Microsoft Vulnerability CVE-2022-21881: A coding deficiency exists in Microsoft Windows Kernel that may lead to elevation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58866 through 58867.
  - Microsoft Vulnerability CVE-2022-21882: A coding deficiency exists in Microsoft Win32k that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58859 through 58860.
  - Microsoft Vulnerability CVE-2022-21887: A coding deficiency exists in Microsoft Win32k that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58874 through 58875.
  - Microsoft Vulnerability CVE-2022-21897: A coding deficiency exists in Microsoft Windows Common Log File System Driver that may lead to an escalation of privilege.
  - Previously released rules will detect attacks targeting these vulnerabilities and have been updated with the appropriate reference information. They are also included in this release and are identified with GID 1, SIDs 40689 through 40690.
  - Microsoft Vulnerability CVE-2022-21907: A coding deficiency exists in HTTP Stack that may lead to remote code execution.
  - Preprocessors to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 119, SIDs 19 and 31.
  - Microsoft Vulnerability CVE-2022-21908: A coding deficiency exists in Microsoft Windows Installer that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58870 through 58871.
  - Microsoft Vulnerability CVE-2022-21916: A coding deficiency exists in Microsoft Windows Common Log File System Driver that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58872 through 58873.
  - Microsoft Vulnerability CVE-2022-21919: A coding deficiency exists in Microsoft Windows User Profile Service that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58868 through 58869.

- Talos also has added and modified multiple rules in the file-other, indicator-obfuscation, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

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

- CVE-2022-22722: (Use of Hard-coded Credentials Vulnerability in Schneider Easergy P5)
  A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration.
- CVE-2022-22723: (Buffer Copy without Checking Size of Input Vulnerability in Schneider Easergy P5)
  A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted.
- CVE-2022-22725: (Buffer Copy without Checking Size of Input Vulnerability in Schneider Easergy P3)
  A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted.
- CVE-2020-8597: (Buffer Copy without Checking Size of Input Vulnerability in Schneider Easergy T300)
  A point-to-point (pppd) communication library deployed with the T300 is vulnerable to CVE-2020-8597, a CWE-120: Buffer Copy without Checking Size of Input vulnerability, which may allow for arbitrary code execution and lead to a denial of service when an attacker gains access to a connected cellular network. The CVSS score, provided above, is evaluated as Medium in the product context.
- CVE-2022-22724: (Uncontrolled Resource Consumption Vulnerability in Schneider Modicon M340 Controller)
  A CWE-400: Uncontrolled Resource Consumption vulnerability exists that could cause a denial of service on ports 80 (HTTP) and 502 (Modbus), when sending a large number of TCP RST or FIN packets to any open TCP port of the PLC.
- CVE-2020-7534: (Cross-Site Request Forgery (CSRF) Vulnerability in Schneider M340 Controller and Communication Modules)
  A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists on the web server used, that could cause a leak of sensitive data or unauthorized actions on the web server during the time the user is logged in.
- CVE-2021-41769: (Information Disclosure Vulnerability in Siemens SIPROTEC 5 Device)
  An improper input validation vulnerability in the web server could allow an unauthenticated user to access device information.
- CVE-2021-45033: (Use of Hard-coded Credentials in Siemens SICAM A8000)
  An undocumented debug port uses hard-coded default credentials. If this port is enabled by a privileged user, an attacker aware of the credentials could access an administrative debug shell on the affected device.
- CVE-2021-45034: (Improper Access Control in Siemens SICAM A8000)
  The web server of the affected system allows access to logfiles and diagnostic data generated by a privileged user. An unauthenticated attacker could access the files by knowing the corresponding download links.
- CVE-2021-30061: (Code Execution Vulnerability via USB In Tofino)
  An attacker can execute code on the Tofino device by attaching a USB stick with a specially crafted file to the device.

- CVE-2021-30062: (OPC Enforcer Bypass In Tofino)
  An attacker can bypass the OPC enforcer using crafted OPC packets.
- CVE-2021-30063: (Denial of Service of the OPC Enforcer In Tofino)
  An attacker can cause a denial of service in the OPC enforcer using crafted OPC packets.
- CVE-2021-30064: (SSH Hardcoded Default Credentials in Tofino)
  An attacker can access an uncommissioned Tofino device using hardcoded default credentials via SSH.
- CVE-2021-30065: (Modbus Enforcer Bypass in Tofino)
  An attacker can bypass the Modbus enforcer using crafted Modbus packets.
- CVE-2021-30066: (Firmware Signature Verification Bypass via USB in Tofino)
  An attacker can bypass firmware signature verification on a USB stick and load arbitrary firmware images on the device.
- CVE-2021-33485: (Out-of-bounds Write In CODESYS V2 web server)
  CODESYS Control Runtime system before 3.5.17.10 is vulnerable to a Out-of-bounds Write. Crafted web server requests may cause invalid memory accesses to crash the CODESYS web server or may read stack or heap memory.
- CVE-2021-29241: (NULL Pointer Dereference In CODESYS Gateway V3)
  CODESYS Gateway 3 before 3.5.16.70 has a NULL pointer dereference that may result in a denial of service (DoS). Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition.

Since November 11, 2022, several CVEs of the Knowledge Data Base have been entered with incorrect matching equipment version numbers, the current release fixes this problem. The following list of CVEs are affected by this problem:

- CVE-2021-37752: (Command Injection for Authentication in Moxa Devices)
  Command Injection for Authentication (CWE-77) vulnerability exist in Moxa devices. An attacker located remotely can execute arbitrary commands on the device via a web interface.
- CVE-2020-28895: (Integer Overflow or Wraparound and Out-of-bounds Write in Wind River VxWorks)
  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-2018-20750: (Out-of-bounds Write in LibVNCServer)
  LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
- CVE-2020-25687: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. This flaw allows a remote attacker, who can create valid DNS replies, to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in sort_rrset() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
- CVE-2020-14398: (Loop with Unreachable Exit Condition in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c.

- CVE-2021-22815: (Information Exposure in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-200: Information Exposure vulnerability exists which could cause the troubleshooting archive to be accessed.
- CVE-2021-22821: (Server-Side Request Forgery (SSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-918 Server-Side Request Forgery (SSRF) vulnerability exists that could cause the station web server to forward requests to unintended network targets when crafted malicious parameters are submitted to the charging station web server.
- CVE-2019-13946: (Uncontrolled Resource Consumption Vulnerability in Siemens PROFINET-IO Stack)
  PROFINET-IO (PNIO) stack versions prior v06.00 do not properly limit internal resource allocation when multiple legitimate Diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial-of-service condition due to lack of memory for devices that include a vulnerable version of the stack.
- CVE-2020-25684: (Authentication Bypass by Spoofing in DNSMasq (DNSpooq))
  A vulnerability exists when getting a reply from a forwarded query, where Dnsmasq checks in forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. This could allow an attacker to perform a DNS cache poisoning attack.
- CVE-2021-40366: (Missing Encryption of Sensitive Data Vulnerability in Siemens Climatix POL909 (AWM module))
  The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.
- CVE-2021-44165: (Remote Code Execution Vulnerability in Siemens POWER METER SICAM Q100)
  The affected firmware contains a buffer overflow vulnerability in the web application that could allow a remote attacker with engineer or admin privileges to potentially perform remote code execution.
- CVE-2021-22813: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to an edit policy file.
- CVE-2020-25684: (Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
- CVE-2019-15690: (Integer Overflow or Wraparound in LibVNCServer)
  A flaw was found in libvncserver. An integer overflow within the HandleCursorShape() function can be exploited to cause a heap-based buffer overflow by tricking a user or application using libvncserver to connect to an unstrusted server and subsequently send cursor shapes with specially crafted dimensions. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

- CVE-2021-22816: (Improper Check for Unusual or Exceptional Conditions vulnerability in Schneider Electric SCADAPack 300E Series RTU)
  A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a Denial of Service of the RTU when receiving a specially crafted request over Modbus, and the RTU is configured as a Modbus server.
- CVE-2021-22818: (Improper Restriction of Excessive Authentication Attempts in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to gain unauthorized access to the charging station web interface by performing brute force attacks.
- CVE-2020-14397: (NULL Pointer Dereference in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has a NULL pointer dereference.
- CVE-2021-37751: (Reveals Sensitive Information to an Unauthorized Actor in Moxa Devices)
  Reveals Sensitive Information to an Unauthorized Actor (CWE-204) vulnerability exist in Moxa devices. An attacker located remotely can obtain sensitive information.
- CVE-2020-25686: (Use of Insufficiently Random Values in DNSMasq (DNSpooq))
  A flaw was found when receiving a query, where Dnsmasq does not check for an existing pending request for the same name and forwards a new request. This could allow an off-path attacker on the network to substantially reduce the number of attempts to forge a reply and have it accepted by Dnsmasq.
- CVE-2019-15681: (Improper Initialization in LibVNC)
  LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.
- CVE-2020-25685: (Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
- CVE-2021-22825: (Exposure of Sensitive Information to an Unauthorized Actor In Schneider Rack Power Distribution Unit)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an attacker to access the system with elevated privileges when a privileged account clicks on a malicious URL that compromises the security token.
- CVE-2020-25685: (Authentication Bypass by Spoofing in DNSMasq (DNSpooq))
  Due to a weak hash, an off-path attacker can find several different domains with the same hash, substantially reducing the number of attempts to forge a reply for acceptance by Dnsmasq. This could allow an attacker to perform a DNS cache poisoning attack.
- CVE-2020-25682: (Out-of-bounds Write and Heap-based Buffer Overflow in dnsmasq)

A flaw was found in dnsmasq before 2.83. A buffer overflow vulnerability was discovered in the way dnsmasq extract names from DNS packets before validating them with DNSSEC data. An attacker on the network, who can create valid DNS replies, could use this flaw to cause an overflow with arbitrary data in a heap-allocated memory, possibly executing code on the machine. The flaw is in the rfc1035.c:extract_name() function, which writes data to the memory pointed by name assuming MAXDNAME*2 bytes are available in the buffer. However, in some code execution paths, it is possible extract_name() gets passed an offset from the base buffer, thus reducing, in practice, the number of available bytes that can be written in the buffer. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

- CVE-2020-14402: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings.
- CVE-2021-22724: (Cross-Site Request Forgery (CSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CVE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could allow an attacker to impersonate the user or carry out actions on their behalf when crafted malicious parameters are submitted in POST requests sent to the charging station web server.
- CVE-2017-18922: (Out-of-bounds Write in LibVNC)
  websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A malicious attacker could exploit this by sending specially crafted WebSocket frames to a server, causing a heap-based buffer overflow.
- CVE-2020-14404: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings.
- CVE-2021-37754: (Improper Restriction of Excessive Authentication Attempts in Moxa Devices)
  Improper Restriction of Excessive Authentication Attempts (CWE-307) vulnerability exist in Moxa devices. An attacker located remotely can use brute force to obtain credentials.
- CVE-2021-22812: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC.
- CVE-2021-22820: (Insufficient Session Expiration in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-614 Insufficient Session Expiration vulnerability exists that could allow an attacker to maintain an unauthorized access over a hijacked session to the charger station web server even after the legitimate user account holder has changed his password.
- CVE-2019-20788: (Integer Overflow or Wraparound in LibVNCServer)
  libvncclient/cursor.c in LibVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.
- CVE-2021-37758: (Improper Verification of Firmware in Moxa Devices)
  Improper Verification of Firmware (CWE-347) vulnerability exist in Moxa devices. An attacker can create malicious firmware for the device.
- CVE-2021-22810: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to a delete policy file.

- CVE-2021-37757: (Improper Restriction That Causes Buffer Overflow in Moxa Devices)
  Improper Restriction That Causes Buffer Overflow (CWE-119) vulnerability exist in Moxa devices. An attacker located remotely can crash the service of the devices.
- CVE-2021-22819: (Improper Restriction of Rendered UI Layers or Frames in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the web interface rendered within iframes.
- CVE-2020-25681: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in the way RRSets are sorted before validating with DNSSEC data. An attacker on the network, who can forge DNS replies such as that they are accepted as valid, could use this flaw to cause a buffer overflow with arbitrary data in a heap memory segment, possibly executing code on the machine. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
- CVE-2020-14403: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via encodings.
- CVE-2018-20748: (Out-of-bounds Write in LibVNC)
  LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c. The fix for CVE-2018-20019 was incomplete.
- CVE-2021-42027: (Improper Certificate Validation Vulnerability in Siemens SINUMERIK Edge)
  The affected software does not properly validate the server certificate when initiating a TLS connection. This could allow an attacker to spoof a trusted entity by interfering in the communication path between the client and the intended server.
- CVE-2021-22811: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause script execution when the request of a privileged account accessing the vulnerable web page is intercepted.
- CVE-2021-22814: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could cause arbitrary script execution when a malicious file is read and displayed.
- CVE-2020-14396: (NULL Pointer Dereference in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference.
- CVE-2019-20840: (Improper Restriction of Operations within the Bounds of a Memory Buffer in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/ws_decode.c can lead to a crash because of unaligned accesses in hybiReadAndDecode.
- CVE-2019-20839: (Buffer Copy without Checking Size of Input in LibVNCServer)
  libvncclient/sockets.c in LibVNCServer before 0.9.13 has a buffer overflow via a long socket filename.
- CVE-2021-37753: (Authentication Bypass and Unencrypted Credentials in Moxa Devices)

Authentication Bypass and Unencrypted Credentials (CWE-303, CWE-256) vulnerability exist in Moxa devices. An attacker located remotely can bypass authentication mechanisms.

- CVE-2020-35198: (Integer Overflow or Wraparound in Wind River VxWorks 7)
  An issue was discovered in Wind River VxWorks 7. 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-2020-14401: (Integer Overflow or Wraparound in LibVNCServer)
  An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow.
- CVE-2021-37756: (Cross-site scripting (XSS) in Moxa Devices)
  Cross-site scripting (XSS) (CWE-79) vulnerability exist in Moxa devices. An attacker located remotely can insert HTML and JavaScript into the system via a web interface.
- CVE-2021-22822: (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an attacker to impersonate the user who manages the charging station or carry out actions on their behalf when crafted malicious parameters are submitted to the charging station web server.
- CVE-2018-21247: (Exposure of Sensitive Information to an Unauthorized Actor in LibVNCClient)
  An issue was discovered in LibVNCServer before 0.9.13. There is an information leak (of uninitialized memory contents) in the libvncclient/rfbproto.c ConnectToRFBRepeater function.
- CVE-2018-20749: (Out-of-bounds Write in LibVNCServer)
  LibVNC before 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
- CVE-2020-25683: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in get_rdata() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
- CVE-2021-37730: (Command Injection Vulnerability in Siemens SCALANCE W1750D)
  A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) command line interface. Successful exploitation could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the system.
- CVE-2018-20019: (Out-of-bounds Write in LibVNC)
  LibVNC before commit a83439b9fbe0f03c48eb94ed05729cb016f8b72f contains multiple heap out-of-bound write vulnerabilities in VNC client code that can result remote code execution.
- CVE-2020-25686: (Authentication Bypass by Spoofing and Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a

successful attack is reduced. The highest threat from this vulnerability is to data integrity.

- CVE-2021-22725: (Cross-Site Request Forgery (CSRF) in Schneider EVlink City / Parking / Smart Wallbox Charging Stations)
  A CWE-352 Cross-Site Request Forgery (CSRF) vulnerability exists that could cause allow an attacker to perform unintended actions when crafted malicious parameters are submitted in GET requests sent to the charging station web server.
- CVE-2021-37755: (Authentication Bypass and Unencrypted Credentials in Moxa Devices)
  Authentication Bypass and Unencrypted Credentials (CWE-303, CWE-256) vulnerability exist in Moxa devices. An attacker located remotely can bypass authentication mechanisms.
- CVE-2020-14405: (Allocation of Resources Without Limits or Throttling in LibVNCClient)
  An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size.

20220107

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

- **Talos Rules 2022-01-06 (https://www.snort.org/advisories/talos-rules-2022-01-06)**
  - References to CVE 2021-44832 have been added to all existing log4j rules for ease of reference for users. Coverage was not updated as there was no need.
  - Talos has added and modified multiple rules in the file-multimedia, indicator-compromise, malware-cnc, malware-other, policy-other, protocol-other 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-2021-37752: (Command Injection for Authentication in Moxa Devices)
  Command Injection for Authentication (CWE-77) vulnerability exist in Moxa devices. An attacker located remotely can execute arbitrary commands on the device via a web interface.
- CVE-2021-37753: (Authentication Bypass and Unencrypted Credentials in Moxa Devices)
  Authentication Bypass and Unencrypted Credentials (CWE-303, CWE-256) vulnerability exist in Moxa devices. An attacker located remotely can bypass authentication mechanisms.
- CVE-2021-37755: (Authentication Bypass and Unencrypted Credentials in Moxa Devices)
  Authentication Bypass and Unencrypted Credentials (CWE-303, CWE-256) vulnerability exist in Moxa devices. An attacker located remotely can bypass authentication mechanisms.
- CVE-2021-37757: (Improper Restriction That Causes Buffer Overflow in Moxa Devices)
  Improper Restriction That Causes Buffer Overflow (CWE-119) vulnerability exist in Moxa devices. An attacker located remotely can crash the service of the devices.
- CVE-2021-37751: (Reveals Sensitive Information to an Unauthorized Actor in Moxa Devices)
  Reveals Sensitive Information to an Unauthorized Actor (CWE-204) vulnerability exist in Moxa devices. An attacker located remotely can obtain sensitive information.
- CVE-2021-37754: (Improper Restriction of Excessive Authentication Attempts in Moxa Devices)
  Improper Restriction of Excessive Authentication Attempts (CWE-307) vulnerability exist in Moxa devices. An attacker located remotely can use brute force to obtain credentials.
- CVE-2021-37756: (Cross-site scripting (XSS) in Moxa Devices)
  Cross-site scripting (XSS) (CWE-79) vulnerability exist in Moxa devices. An attacker located remotely can

insert HTML and JavaScript into the system via a web interface.

- CVE-2021-37758: (Improper Verification of Firmware in Moxa Devices)
  Improper Verification of Firmware (CWE-347) vulnerability exist in Moxa devices. An attacker can create malicious firmware for the device.
- CVE-2020-25681: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in the way RRSets are sorted before validating with DNSSEC data. An attacker on the network, who can forge DNS replies such as that they are accepted as valid, could use this flaw to cause a buffer overflow with arbitrary data in a heap memory segment, possibly executing code on the machine. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
- CVE-2020-25682: (Out-of-bounds Write and Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before 2.83. A buffer overflow vulnerability was discovered in the way dnsmasq extract names from DNS packets before validating them with DNSSEC data. An attacker on the network, who can create valid DNS replies, could use this flaw to cause an overflow with arbitrary data in a heap-allocated memory, possibly executing code on the machine. The flaw is in the rfc1035.c:extract_name() function, which writes data to the memory pointed by name assuming MAXDNAME*2 bytes are available in the buffer. However, in some code execution paths, it is possible extract_name() gets passed an offset from the base buffer, thus reducing, in practice, the number of available bytes that can be written in the buffer. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
- CVE-2020-25683: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in get_rdata() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
- CVE-2020-25684: (Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
- CVE-2020-25685: (Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.

- CVE-2020-25686: (Authentication Bypass by Spoofing and Improperly Implemented Security Check for Standard in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
- CVE-2020-25687: (Heap-based Buffer Overflow in dnsmasq)
  A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. This flaw allows a remote attacker, who can create valid DNS replies, to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in sort_rrset() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.

The vulnerabilities related to the Omron manufacturer are now supported in the Cisco Cyber Vision Knowledge Data Base. This release also adds support and modifications for the detection of the following old vulnerabilities related to the Omron constructor:

- CVE-2014-2369: (Cross-Site Request Forgery Vulnerability in Omron NS Series HMI)
  The web application receives a request from a client without adequately verifying that the request was intentionally sent. This could allow an attacker to execute commands thereby compromising the system and enabling modifications to the system's configuration.
- CVE-2014-2370: (Cross-Site Scripting Vulnerability in Omron NS Series HMI)
  The web application stores untrusted data that are read back into the application and included in dynamic content.
- CVE-2015-0987: (Cleartext Transmission of Sensitive Information in Omron CJ2M and CJ2H Series PLC)
  The password is transmitted in clear text to unlock the PLC for modification, which leaves the password vulnerable to packet sniffing.
- CVE-2015-1015: (Storing Passwords in a Recoverable Format in Omron CJ2M and CJ2H Series PLC)
  Passwords are locally stored in an object file that is saved in a Compact Flash Card in a recoverable format.
- CVE-2019-18261: (Improper restriction of Excessive Authentication Attempts in Omron CJ, CS and NJ Series PLC)
  The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.
- CVE-2019-18259: (Authentication Bypass by Spoofing in Omron PLC CJ and CS Series)
  An attacker could spoof arbitrary messages or execute commands.
- CVE-2019-13533: (Authentification Bypass by Capture-Replay in Omron PLC CJ and CS Series)
  An attacker could monitor traffic between the PLC and the controller, and replay requests that could result in the opening and closing of industrial valves.
- CVE-2019-18269: (Unrestricted externally Accesible Lock in Omron PLC CJ and CS Series)
  The software properly checks for the existence of a lock, but the lock can be externally controlled or influenced by an actor that is outside of the intended sphere of control.
- CVE-2020-6986: (Uncontrolled Ressource Consumption in Omron PLC CJ Series)
  An attacker can send a series of specific data packets within a short period, causing a service error on the

PLC Ethernet module, which in turn causes a PLC service denied result.