Release Notes for Cisco Cyber Vision Knowledge DB

Release 202202

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.202202	**Description**
CiscoCyberVision_knowledgedb_20220204.db	Knowledge DB version 20220204
CiscoCyberVision_knowledgedb_20220211.db	Knowledge DB version 20220211
CiscoCyberVision_knowledgedb_20220218.db	Knowledge DB version 20220218
CiscoCyberVision_knowledgedb_20220225.db	Knowledge DB version 20220225

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

20220225

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

- **Talos Rules 2022-02-24 (https://www.snort.org/advisories/talos-rules-2022-02-24-2-24-2022)**
  - Talos is releasing Snort coverage for the Cyclops Blink and Hermetic Wiper malware campaigns. The new Snort rules provide protection against the samples related to these two campaigns. SIDs 59095-59098 provide protection against the Cyclops Blink campaign, and SIDs 59099-59100 provide protection against the Hermetic Wiper campaign.
  - Talos has added and modified multiple rules in the malware-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-02-24 (https://www.snort.org/advisories/talos-rules-2022-02-24)**
  - Talos has added and modified multiple rules in the malware-other, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-02-22 (https://www.snort.org/advisories/talos-rules-2022-02-22)**
  - Talos has added and modified multiple rules in the 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-2021-43323: (Improper Input Validation in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in UsbCoreDxe in Insyde InsydeH2O with kernel 5.5 before 05.51.45, 5.4 before 05.43.45, 5.3 before 05.35.45, 5.2 before 05.26.45, 5.1 before 05.16.45, and 5.0 before 05.08.45. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-45970: (Buffer Copy without Checking Size of Input in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in IdeBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the status code saved at the CommBuffer+4 location).
- CVE-2022-24069: (Improper Input Validation in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.0 before 05.08.41, 5.1 before 05.16.29, 5.2 before 05.26.29, 5.3 before 05.35.29, 5.4 before 05.43.29, and 5.5 before 05.51.29. An SMM callout vulnerability allows an attacker to hijack the execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-41841: (Inclusion of Functionality from Untrusted Control Sphere in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.
- CVE-2021-41839: (NULL Pointer Dereference in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write

fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.

- CVE-2020-5953: (Untrusted Pointer Dereference in Siemens SIMATIC IPC and SIMATIC Field PG)
  A vulnerability exists in System Management Interrupt (SWSMI) handler of InsydeH2O UEFI Firmware code located in SWSMI handler that dereferences gRT (EFI_RUNTIME_SERVICES) pointer to call a GetVariable service, which is located outside of SMRAM. This can result in code execution in SMM (escalating privilege from ring 0 to ring -2).
- CVE-2021-45971: (Buffer Copy without Checking Size of Input in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in SdHostDriver in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (CommBufferData).
- CVE-2021-42113: (Improper Input Validation in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in StorageSecurityCommandDxe in Insyde InsydeH2O with Kernel 5.1 before 05.14.28, Kernel 5.2 before 05.24.28, and Kernel 5.3 before 05.32.25. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2022-24030: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2020-27339: (Improper Privilege Management in Siemens SIMATIC IPC and SIMATIC Field PG)
  In the kernel in Insyde InsydeH2O 5.x, certain SMM drivers did not correctly validate the CommBuffer and CommBufferSize parameters, allowing callers to corrupt either the firmware or the OS memory. The fixed versions for this issue in the AhciBusDxe, IdeBusDxe, NvmExpressDxe, SdHostDriverDxe, and SdMmcDeviceDxe drivers are 05.16.25, 05.26.25, 05.35.25, 05.43.25, and 05.51.25 (for Kernel 5.1 through 5.5).
- CVE-2021-33627: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Insyde InsydeH2O 5.x, affecting FwBlockServiceSmm. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses.
- CVE-2021-42059: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Insyde InsydeH2O Kernel 5.0 before 05.08.41, Kernel 5.1 before 05.16.41, Kernel 5.2 before 05.26.41, Kernel 5.3 before 05.35.41, and Kernel 5.4 before 05.42.20. A stack-based buffer overflow leads toarbitrary code execution in UEFI DisplayTypeDxe DXE driver.
- CVE-2021-42554: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Insyde InsydeH2O with Kernel 5.0 before 05.08.42, Kernel 5.1 before 05.16.42, Kernel 5.2 before 05.26.42, Kernel 5.3 before 05.35.42, Kernel 5.4 before 05.42.51, and Kernel 5.5 before 05.50.51. An SMM memory corruption vulnerability in FvbServicesRuntimeDxe allows a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-41840: (Allocation of Resources Without Limits or Throttling in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.

- CVE-2021-33625: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Kernel 5.x in Insyde InsydeH2O, affecting HddPassword. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses.
- CVE-2021-41837: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-41838: (Improper Restriction of Operations within the Bounds of a Memory Buffer in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in SdHostDriver in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of a Numeric Range Comparison Without a Minimum Check.
- CVE-2021-33626: (Inclusion of Functionality from Untrusted Control Sphere in Siemens SIMATIC IPC and SIMATIC Field PG)
  In the kernel in Insyde InsydeH2O 5.x, certain SMM drivers did not correctly validate the CommBuffer and CommBufferSize parameters, allowing callers to corrupt either the firmware or the OS memory. The fixed versions for this issue in the PnpSmm, SmmResourceCheckDxe, and BeepStatusCode drivers are 05.08.23, 05.16.23, 05.26.23, 05.35.23, 05.43.23, and 05.51.23 (for Kernel 5.0 through 5.5).
- CVE-2021-42060: (Improper Input Validation in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Insyde InsydeH2O Kernel 5.0 through 05.08.41, Kernel 5.1 through 05.16.41, Kernel 5.2 before 05.23.22, and Kernel 5.3 before 05.32.22. An Int15ServiceSmm SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-45969: (Buffer Copy without Checking Size of Input in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 before 05.16.25, 5.2 before 05.26.25, 5.3 before 05.35.25, 5.4 before 05.43.25, and 5.5 before 05.51.25. A vulnerability exists in the SMM (System Management Mode) branch that registers a SWSMI handler that does not sufficiently check or validate the allocated buffer pointer (the CommBuffer+8 location).
- CVE-2021-43522: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in Insyde InsydeH2O with kernel 5.1 through 2021-11-08, 5.2 through 2021-11-08, and 5.3 through 2021-11-08. A StorageSecurityCommandDxe SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2022-24031: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in NvmExpressDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2021-43615: (Out-of-bounds Write in Siemens SIMATIC IPC and SIMATIC Field PG)
  An issue was discovered in HddPassword in Insyde InsydeH2O with kernel 5.1 before 05.16.23, 5.2 before 05.26.23, 5.3 before 05.35.23, 5.4 before 05.43.22, and 5.5 before 05.51.22. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.
- CVE-2020-1301: (Windows SMB Remote Code Execution Vulnerability)

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server..

- CVE-2022-20625: (Cisco FXOS and NX-OS Software Cisco Discovery Protocol Service Denial of Service Vulnerability)
  A vulnerability in the Cisco Discovery Protocol service of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the service to restart, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of Cisco Discovery Protocol messages that are processed by the Cisco Discovery Protocol service. An attacker could exploit this vulnerability by sending a series of malicious Cisco Discovery Protocol messages to an affected device. A successful exploit could allow the attacker to cause the Cisco Discovery Protocol service to fail and restart. In rare conditions, repeated failures of the process could occur, which could cause the entire device to restart.
- CVE-2022-20624: (Cisco NX-OS Software Cisco Fabric Services Over IP Denial of Service Vulnerability)
  A vulnerability in the Cisco Fabric Services over IP (CFSoIP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of incoming CFSoIP packets. An attacker could exploit this vulnerability by sending crafted CFSoIP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.
- CVE-2022-20623: (Cisco Nexus 9000 Series Switches Bidirectional Forwarding Detection Denial of Service Vulnerability)
  A vulnerability in the rate limiter for Bidirectional Forwarding Detection (BFD) traffic of Cisco NX-OS Software for Cisco Nexus 9000 Series Switches could allow an unauthenticated, remote attacker to cause BFD traffic to be dropped on an affected device. This vulnerability is due to a logic error in the BFD rate limiter functionality. An attacker could exploit this vulnerability by sending a crafted stream of traffic through the device. A successful exploit could allow the attacker to cause BFD traffic to be dropped, resulting in BFD session flaps. BFD session flaps can cause route instability and dropped traffic, resulting in a denial of service (DoS) condition. This vulnerability applies to both IPv4 and IPv6 traffic.
- CVE-2022-20650: (Cisco NX-OS Software NX-API Command Injection Vulnerability)
  A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation of user supplied data that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP POST request to the NX-API of an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. Note: The NX-API feature is disabled by default.

20220218

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

- **Talos Rules 2022-02-17 (https://www.snort.org/advisories/talos-rules-2022-02-17)**
  - Talos has added and modified multiple rules in the deleted, file-other, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-02-15 (https://www.snort.org/advisories/talos-rules-2022-02-15)**

- Talos has added and modified multiple rules in the browser-other, malware-other, os-windows, policy-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-2021-1529: (Cisco IOS XE SD-WAN Software Command Injection Vulnerability)
  A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges. The vulnerability is due to insufficient input validation by the system CLI. An attacker could exploit this vulnerability by authenticating to an affected device and submitting crafted input to the system CLI. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.

20220211

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

- **Talos Rules 2022-02-10 (https://www.snort.org/advisories/talos-rules-2022-02-10)**
  - Talos has added and modified multiple rules in the file-image, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-02-08 (https://www.snort.org/advisories/talos-rules-2022-02-08)**
  - Microsoft Vulnerability CVE-2022-21989: 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 59001 through 59002.
  - Microsoft Vulnerability CVE-2022-21994: A coding deficiency exists in Microsoft DWM Core Library 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 58999 through 59000.
  - Microsoft Vulnerability CVE-2022-21996: 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 59008 through 59009.
  - Microsoft Vulnerability CVE-2022-22000: 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 59006 through 59007.
  - Microsoft Vulnerability CVE-2022-22715: A coding deficiency exists in Named Pipe File System 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 59004 through 59005.
  - Microsoft Vulnerability CVE-2022-22718: A coding deficiency exists in Microsoft Windows Print Spooler 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 58993 through 58994.
- Talos also has added and modified multiple rules in the file-executable, file-image, malware-cnc, os-windows, policy-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-2022-22813: (Use of Hard-coded Credentials Vulnerability in Schneider Easergy P40)
  A CWE-798: Use of Hard-coded Credentials vulnerability exists. If an attacker were to obtain the TLS cryptographic key and take active control of the Courier tunneling communication network, they could potentially observe and manipulate traffic associated with product configuration.
- CVE-2021-22817: (Incorrect Default Permissions vulnerability in Schneider Harmony/Magelis iPC Series HMI)
  A CWE-276: Incorrect Default Permissions vulnerability exists that could cause unauthorized access to the base installation directory leading to local privilege escalation.
- CVE-2022-22810: (Improper Restriction of Excessive Authentication Attempts Vulnerability in Schneider SpaceLYnk, Wiser For KNX, and FellerLYnk Products)
  A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to manipulate the admin after numerous attempts at guessing credentials.
- CVE-2022-22809: (Missing Authentication for Critical Function Vulnerability in Schneider SpaceLYnk, Wiser For KNX, and FellerLYnk Products)
  A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow modifications of the touch configurations in an unauthorized manner when an attacker attempts to modify the touch configurations.
- CVE-2022-22812: (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability in Schneider SpaceLYnk, Wiser For KNX, and FellerLYnk Products)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a web session compromise when an attacker injects and then executes arbitrary malicious JavaScript code inside the target browser.
- CVE-2022-22811: (Cross-Site Request Forgery (CSRF) Vulnerability in Schneider SpaceLYnk, Wiser For KNX, and FellerLYnk Products)
  A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists that could induce users to perform unintended actions, leading to the override of the system's configurations when an attacker persuades a user to visit a rogue website.
- CVE-2022-22807: (Improper Restriction of Rendered UI Layers or Frames Vulnerability in Schneider EcoStruxure EV Charging Expert)
  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-2022-22808: (Permissive Cross-domain Policy with Untrusted Domains Vulnerability in Schneider EcoStruxure EV Charging Expert)
  A CWE-942: Permissive Cross-domain Policy with Untrusted Domains vulnerability exists that could cause a remote attacker to gain unauthorized access to the product when conducting cross-domain attacks based on same-origin policy or cross-site request forgery protections bypass.
- CVE-2021-37204: (Denial of Service Vulnerabilities in Siemens SIMATIC Devices)
  An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially

prepared packet over port 102/tcp. A restart of the affected device is needed to restore normal operations.

- CVE-2021-37185: (Denial of Service Vulnerabilities in Siemens SIMATIC Devices)
  An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.
- CVE-2021-37205: (Denial of Service Vulnerabilities in Siemens SIMATIC Devices)
  An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.
- CVE-2021-3712: (OpenSSL - Read buffer overruns processing ASN.1 strings Vulnerability)
  ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).
- CVE-2021-41991: (StrongSwan - Integer Overflow or Wraparound Vulnerability)
  The in-memory certificate cache in strongSwan before version 5.9.4 has a remote integer overflow vulnerability upon receiving many requests with different certificates to fill the cache and later trigger the replacement of cache entries. The code attempts to select a less-often-used cache entry by means of a random number generator, but this is not done correctly. This could lead to a denial of service (DoS) condition. Remote code execution can't be excluded completely, but it would require attackers to have control over the dereferenced memory, so it is very unlikely
- CVE-2021-41990: (StrongSwan - Integer Overflow or Wraparound Vulnerability)
  The gmp plugin in strongSwan before version 5.9.4 has a remote integer overflow vulnerability via a crafted certificate with an RSASSA-PSS signature. For example, this can be triggered by an unrelated self-signed CA certificate sent by an initiator. Remote code execution cannot occur.

20220204

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

- **Talos Rules 2022-02-03 (https://www.snort.org/advisories/talos-rules-2022-02-03)**
  - Talos has added and modified multiple rules in the indicator-shellcode and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-02-01 (https://www.snort.org/advisories/talos-rules-2022-02-01)**
  - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.