Release Notes for Cisco Cyber Vision Knowledge DB

Release 202204

Compatible device list 2

Links 2

Software Download 2

Related Documentation 2

Database download 3

How to update the database 3

Release contents 4

20220429 4

20220422 4

20220415 4

20220408 10

20220401 11

Compatible device list

Center	Description
All version 4 centers	All Cisco Cyber Vision center version 4 are compatible with this Knowledge DB file.

Links

Software Download

The files listed below can be found using the following link:

https://software.cisco.com/download/home/286325414/type

Center	Description
CiscoCyberVision-center-4.1.0.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-4.1.0.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-4.1.0.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-4.1.0.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-4.1.0.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-4.1.0.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-4.1.0.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-4.1.0.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	**Description**
CiscoCyberVision-Embedded-KDB-4.1.0.dat	Knowledge DB embedded in Cisco Cyber Vision 4.1.0
Updates/KDB/KDB.202204	**Description**
CiscoCyberVision_knowledgedb_20220401.db	Knowledge DB version 20220401
CiscoCyberVision_knowledgedb_20220408.db	Knowledge DB version 20220408
CiscoCyberVision_knowledgedb_20220415.db	Knowledge DB version 20220415
CiscoCyberVision_knowledgedb_20220422.db	Knowledge DB version 20220422
CiscoCyberVision_knowledgedb_20220429.db	Knowledge DB version 20220429

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

20220429

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

- **Talos Rules 2022-04-28 (https://www.snort.org/advisories/talos-rules-2022-04-28)**
  - Talos has added and modified multiple rules in the file-office, file-other, os-windows, policy-other, protocol-dns, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-04-26 (https://www.snort.org/advisories/talos-rules-2022-04-26)**
  - Talos has added and modified multiple rules in the file-flash, file-pdf, malware-cnc, os-windows and server-other rule sets to provide coverage for emerging threats from these technologies.

20220422

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

- **Talos Rules 2022-04-21 (https://www.snort.org/advisories/talos-rules-2022-04-21)**
  - Talos has added and modified multiple rules in the file-other, malware-cnc, protocol-dns, protocol-voip and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-04-19 (https://www.snort.org/advisories/talos-rules-2022-04-19)**
  - Talos has added and modified multiple rules in the file-multimedia, file-office, file-other, protocol-dns, protocol-imap, server-oracle and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220415

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

- **Talos Rules 2022-04-14 (https://www.snort.org/advisories/talos-rules-2022-04-14)**
  - Talos has added and modified multiple rules in the browser-other, file-image, file-java, file-other, os-windows, protocol-dns, protocol-other, protocol-scada and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-04-12 (https://www.snort.org/advisories/talos-rules-2022-04-12)**
  - Microsoft Vulnerability CVE-2022-24474: 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 59497 through 59498.
  - Microsoft Vulnerability CVE-2022-24481: 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 59521 through 59522.
  - Microsoft Vulnerability CVE-2022-24491: A coding deficiency exists in Microsoft Windows Network File System that may lead to remote code execution.

    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 59534 through 59535.
- Microsoft Vulnerability CVE-2022-24497: A coding deficiency exists in Microsoft Windows Network File System that may lead to remote code execution.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 59533.
- Microsoft Vulnerability CVE-2022-24521: 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 59523 through 59524.
- Microsoft Vulnerability CVE-2022-24542: 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 59525 through 59526.
- Microsoft Vulnerability CVE-2022-24546: 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 59529 through 59530.
- Microsoft Vulnerability CVE-2022-24547: A coding deficiency exists in Microsoft Windows Digital Media Receiver 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 59531 through 59532.
- Microsoft Vulnerability CVE-2022-26904: 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 59511 through 59512.
- Microsoft Vulnerability CVE-2022-26914: 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 59519 through 59520.
- Talos also has added and modified multiple rules in the file-image, file-other, malware-cnc, os-windows, protocol-ftp, protocol-other, protocol-scada, pua-other, server-apache 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-2022-25753: (Use of Insufficiently Random Values Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - The handling of arguments such as IP addresses in the CLI of affected devices is prone to buffer overflows. This could allow an authenticated remote attacker to execute arbitrary code on the device.
- CVE-2022-27481: (Multiple Denial Of Service Vulnerabilities in Siemens SCALANCE W1700 Devices)
    - Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.
- CVE-2022-26334: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)

    - Affected devices do not properly validate the GET parameter XNo of incoming HTTP requests. This could allow an unauthenticated remote attacker to crash affected devices.
  - CVE-2022-25754: (Cross-Site Request Forgery Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - The integrated web server of the affected device could allow remote attackers to perform actions with the permissions of a victim user, provided the victim user has an active session and is induced to trigger the malicious request.
  - CVE-2022-26335: (Classic Buffer Overflow Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.
  - CVE-2022-28328: (Multiple Denial Of Service Vulnerabilities in Siemens SCALANCE W1700 Devices)
    - Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.
  - CVE-2022-25622: (Denial of Service Vulnerability in PROFINET Stack Integrated on Interniche Stack)
    - The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, contains a vulnerability that could allow an attacker to cause a denial of service condition on affected industrial products.
  - CVE-2022-28329: (Multiple Denial Of Service Vulnerabilities in Siemens SCALANCE W1700 Devices)
    - Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.
  - CVE-2022-25751: (Improper Input Validation Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - Affected devices do not properly validate the HTTP headers of incoming requests. This could allow an unauthenticated remote attacker to crash affected devices
  - CVE-2022-25756: (Basic XSS Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. This can be used by an attacker to trigger a malicious request on the affected device.
  - CVE-2022-26380: (Out-of-bounds Read Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - Affected devices do not properly validate the URI of incoming HTTP GET requests. This could allow an unauthenticated remote attacker to crash affected devices.
  - CVE-2022-27480: (Unauthenticated File Access Vulnerability in Siemens SICAM A8000 Devices)
    - SICAM A8000 CP-8050 and CP-8031 devices contain vulnerabilities that could allow an attacker to access files without authentication. For both SICAM A8000 CP-8031 and SICAM A8000 CP-8050, please update to V4.80 or later version
  - CVE-2022-25752: (Use of Insufficiently Random Values Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions
  - CVE-2022-25755: (Improper Access Control Vulnerability in Siemens SCALANCE X-300 Switch Family Devices)
    - The webserver of an affected device is missing specific security headers. This could allow an remote attacker to extract confidential session information under certain circumstances.
  - CVE-2022-0222: (Improper Privilege Management Vulnerability in Modicon M340 Controller and Communication Modules)
    - An improper privilege management vulnerability exists that could cause a denial of service of the Ethernet communication of the controller when sending a specific request over SNMP.
  - CVE-2022-20722: (Cisco IOx Application Hosting Environment Vulnerabilities)

    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20692: (Cisco IOS XE Software NETCONF Over SSH Denial of Service Vulnerability)
    - A vulnerability in the NETCONF over SSH feature of Cisco IOS XE Software could allow a low-privileged, authenticated, remote attacker to cause a denial of service condition (DoS) on an affected device. This vulnerability is due to insufficient resource management. An attacker could exploit this vulnerability by initiating a large number of NETCONF over SSH connections. A successful exploit could allow the attacker to exhaust resources, causing the device to reload and resulting in a DoS condition on an affected device.
  - CVE-2022-20719: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20679: (Cisco IOS XE Software IPSec Denial of Service Vulnerability)
    - A vulnerability in the IPSec decryption routine of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to buffer exhaustion that occurs while traffic on a configured IPsec tunnel is being processed. An attacker could exploit this vulnerability by sending traffic to an affected device that has a maximum transmission unit (MTU) of 1800 bytes or greater. A successful exploit could allow the attacker to cause the device to reload.
  - CVE-2022-20718: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20758: (Cisco IOS XR Software Border Gateway Protocol Ethernet VPN Denial of Service Vulnerability)
    - A vulnerability in the implementation of the Border Gateway Protocol (BGP) Ethernet VPN (EVPN) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to the incorrect processing of a BGP update message that contains specific EVPN attributes. An attacker could exploit this vulnerability by sending a BGP update message that contains specific EVPN attributes. To exploit this vulnerability, an attacker must control a BGP speaker that has an established trusted peer connection to an affected device that is configured with the address family L2VPN EVPN to receive and process the update message. This vulnerability cannot be exploited by any data that is initiated by clients on the Layer 2 network or by peers that are not configured to accept the L2VPN EVPN address family. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition.
  - CVE-2022-20726: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install

applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.

- CVE-2022-20724: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
- CVE-2022-20697: (Cisco IOS and IOS XE Software Web Services Denial of Service Vulnerability)
    - A vulnerability in the web services interface of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper resource management in the HTTP server code. An attacker could exploit this vulnerability by sending a large number of HTTP requests to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2022-20725: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
- CVE-2022-20676: (Cisco IOS XE Software Tool Command Language Privilege Escalation Vulnerability)
    - A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS XE Software could allow an authenticated, local attacker to escalate from privilege level 15 to root-level privileges. This vulnerability is due to insufficient input validation of data that is passed into the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to execute arbitrary commands as root. By default, Tcl shell access requires privilege level 15.
- CVE-2022-20683: (Cisco IOS XE Software for Catalyst 9800 Series Wireless Controllers Application Visibility and Control Denial of Service Vulnerability)
    - A vulnerability in the Application Visibility and Control (AVC-FNF) feature of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient packet verification for traffic inspected by the AVC feature. An attacker could exploit this vulnerability by sending crafted packets from the wired network to a wireless client, resulting in the crafted packets being processed by the wireless controller. A successful exploit could allow the attacker to cause a crash and reload of the affected device, resulting in a DoS condition.
- CVE-2022-20714: (Cisco IOS XR Software for ASR 9000 Series Routers Lightspeed-Plus Line Cards Denial of Service Vulnerability)
    - A vulnerability in the data plane microcode of Lightspeed-Plus line cards for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause the line card to reset. This vulnerability is due to the incorrect handling of malformed packets that are received on the Lightspeed-Plus line cards. An attacker could exploit this vulnerability by sending a crafted IPv4 or IPv6 packet through an affected device. A successful exploit could allow the attacker to cause the Lightspeed-Plus line card to reset, resulting in a denial of service (DoS) condition for any traffic that traverses that line card.
- CVE-2022-20723: (Cisco IOx Application Hosting Environment Vulnerabilities)

    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20721: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20684: (Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family SNMP Trap Denial of Service Vulnerability)
    - A vulnerability in Simple Network Management Protocol (SNMP) trap generation for wireless clients of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, adjacent attacker to cause an affected device to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. This vulnerability is due to a lack of input validation of the information used to generate an SNMP trap related to a wireless client connection event. An attacker could exploit this vulnerability by sending an 802.1x packet with crafted parameters during the wireless authentication setup phase of a connection. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
  - CVE-2022-20677: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20681: (Cisco IOS XE Software for Cisco Catalyst 9000 Family Switches and Catalyst 9000 Family Wireless Controllers Privilege Escalation Vulnerability)
    - A vulnerability in the CLI of Cisco IOS XE Software for Cisco Catalyst 9000 Family Switches and Cisco Catalyst 9000 Family Wireless Controllers could allow an authenticated, local attacker to elevate privileges to level 15 on an affected device. This vulnerability is due to insufficient validation of user privileges after the user executes certain CLI commands. An attacker could exploit this vulnerability by logging in to an affected device as a low-privileged user and then executing certain CLI commands. A successful exploit could allow the attacker to execute arbitrary commands with level 15 privileges on the affected device.
  - CVE-2022-20727: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.
  - CVE-2022-20720: (Cisco IOx Application Hosting Environment Vulnerabilities)
    - Multiple vulnerabilities in the Cisco IOx application hosting environment on multiple Cisco platforms could allow an attacker to inject arbitrary commands into the underlying host operating system, execute arbitrary code on the underlying host operating system, install applications without being authenticated, or conduct a cross-site scripting (XSS) attack against a user of the affected software.

- CVE-2022-20761: (Cisco 1000 Series Connected Grid Router Integrated Wireless Access Point Denial of Service Vulnerability)
    - A vulnerability in the integrated wireless access point (AP) packet processing of the Cisco 1000 Series Connected Grid Router (CGR1K) could allow an unauthenticated, adjacent attacker to cause a denial-of-service condition on an affected device. This vulnerability is due to insufficient input validation of received traffic. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the integrated AP to stop processing traffic, resulting in a DoS condition. It may be necessary to manually reload the CGR1K to restore AP operation.
- CVE-2022-20694: (Cisco IOS XE Software Border Gateway Protocol Resource Public Key Infrastructure Denial of Service Vulnerability)
    - A vulnerability in the implementation of the Resource Public Key Infrastructure (RPKI) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the Border Gateway Protocol (BGP) process to crash, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of a specific RPKI to Router (RTR) Protocol packet header. An attacker could exploit this vulnerability by compromising the RPKI validator server and sending a specifically crafted RTR packet to an affected device. Alternatively, the attacker could use man-in-the-middle techniques to impersonate the RPKI validator server and send a crafted RTR response packet over the established RTR TCP connection to the affected device. A successful exploit could allow the attacker to cause a DoS condition because the BGP process could constantly restart and BGP routing could become unstable.
- CVE-2022-20682: (Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Denial of Service Vulnerability)
    - A vulnerability in the Control and Provisioning of Wireless Access Points (CAPWAP) protocol processing of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to inadequate input validation of incoming CAPWAP packets encapsulating multicast DNS (mDNS) queries. An attacker could exploit this vulnerability by connecting to a wireless network and sending a crafted mDNS query, which would flow through and be processed by the wireless controller. A successful exploit could allow the attacker to cause the affected device to crash and reload, resulting in a DoS condition.
- CVE-2022-20678: (Cisco IOS XE Software AppNav-XE Denial of Service Vulnerability)
    - A vulnerability in the AppNav-XE feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of certain TCP segments. An attacker could exploit this vulnerability by sending a stream of crafted TCP traffic at a high rate through an interface of an affected device. That interface would need to have AppNav interception enabled. A successful exploit could allow the attacker to cause the device to reload.
- CVE-2022-20693: (Cisco IOS XE Software Web UI API Injection Vulnerability)
    - A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI API. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.

20220408

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

- **Talos Rules 2022-04-07 (https://www.snort.org/advisories/talos-rules-2022-04-07)**
    - Talos has added and modified multiple rules in the file-image, file-office, file-other, file-pdf, indicator-obfuscation, indicator-shellcode, protocol-scada and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-04-05 (https://www.snort.org/advisories/talos-rules-2022-04-05)**
    - Talos has added and modified multiple rules in the browser-chrome, file-multimedia, file-other, malware-cnc, malware-other, os-other, os-windows, protocol-scada, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20220401

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

- **Talos Rules 2022-03-31 (https://www.snort.org/advisories/talos-rules-2022-03-31)**
    - Talos has added and modified multiple rules in the exploit-kit, file-office, os-windows, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-03-29 (https://www.snort.org/advisories/talos-rules-2022-03-29)**
    - Talos has added and modified multiple rules in the browser-ie, malware-cnc, malware-other, policy-social, policy-spam, protocol-scada, protocol-telnet 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-2022-1159: (Code Injection Vulnerability in Rockwell Automation Studio 5000 Logix Designer)
    - An attacker who achieves administrator access on a workstation running Studio 5000 Logix Designer could inject controller code undetectable to a user.
- CVE-2022-1161: (Inclusion of Functionality from Untrusted Control Sphere Vulnerability in Rockwell Automation Logix Controllers)
    - An attacker with the ability to modify a user program may change user program code on some ControlLogix, CompactLogix, and GuardLogix Control systems. Studio 5000 Logix Designer writes user-readable program code to a separate location than the executed compiled code, allowing an attacker to change one and not the other.