Release Notes for Cisco Cyber Vision Knowledge DB

Release 202210

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.202210	**Description**
CiscoCyberVision_knowledgedb_20221007.db	Knowledge DB version 20221007
CiscoCyberVision_knowledgedb_20221014.db	Knowledge DB version 20221014
CiscoCyberVision_knowledgedb_20221021.db	Knowledge DB version 20221021
CiscoCyberVision_knowledgedb_20221028.db	Knowledge DB version 20221028

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

20221028

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

- **Talos Rules 2022-10-27 (https://www.snort.org/advisories/talos-rules-2022-10-27)**
    - Talos has added and modified multiple rules in the and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-10-25 (https://www.snort.org/advisories/talos-rules-2022-10-25)**
    - Talos has added and modified multiple rules in the file-image, file-other, malware-cnc, malware-other, os-linux, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20221021

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

- **Talos Rules 2022-10-20 (https://www.snort.org/advisories/talos-rules-2022-10-20)**
    - Talos has added and modified multiple rules in the malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies
- **Talos Rules 2022-10-18 (https://www.snort.org/advisories/talos-rules-2022-10-18)**
    - Talos has added and modified multiple rules in the file-image, malware-cnc, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20221014

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

- **Talos Rules 2022-10-13 (https://www.snort.org/advisories/talos-rules-2022-10-13)**
    - Talos has added and modified multiple rules in the file-image, file-java and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-10-11 (https://www.snort.org/advisories/talos-rules-2022-10-11)**
    - Microsoft Vulnerability CVE-2022-37970: 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: Snort 2: GID 1, SIDs 60698 through 60699, Snort 3: GID 1, SID 300292.
    - Microsoft Vulnerability CVE-2022-37974: A coding deficiency exists in Microsoft Windows Mixed Reality Developer Tools that may lead to information disclosure.
        - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60700 through 60701, Snort 3: GID 1, SID 300293.

- Microsoft Vulnerability CVE-2022-37987: A coding deficiency exists in Microsoft Windows Active Directory Certificate Services that may lead to security feature bypass.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60706 through 60707, Snort 3: GID 1, SID 300297.
- Microsoft Vulnerability CVE-2022-37989: A coding deficiency exists in Microsoft Windows Client Server Run-time Subsystem (CSRSS) that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60704 through 60705, Snort 3: GID 1, SID 300296.
- Microsoft Vulnerability CVE-2022-38050: 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: Snort 2: GID 1, SIDs 60693 through 60696, Snort 3: GID 1, SIDs 300290 through 300291.
- Microsoft Vulnerability CVE-2022-38051: A coding deficiency exists in Microsoft Graphics Component that may lead to an escalation of privilege.
    - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with: Snort 2: GID 1, SIDs 60708 through 60709, Snort 3: GID 1, SID 300298.
- Talos also has added and modified multiple rules in the browser-ie, file-identify 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 vulnerability:

- CVE-2022-38465: (Weak Key Protection Vulnerability in Siemens SIMATIC S7-1200 and S7-1500 CPU Families)
    - SIMATIC S7-1200, S7-1500 CPUs and related products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.
- CVE-2022-36360: (Firmware Authenticity Vulnerability in Siemens LOGO! 8 BM Devices)
    - LOGO! 8 BM (incl. SIPLUS variants) contains a vulnerability that could allow an attacker to install manipulated firmware packages.
- CVE-2022-38371: (Uncontrolled Resource Consumption in Siemens APOGEE, TALON and Desigo PXC/PXM Products)
    - A denial-of-service vulnerability has been identified in in FTP Server of Nucleus RTOS based APOGEE, TALON and Desigo PXC/PXM Products

- CVE-2022-36363: (Improper Input Validation Vulnerability in Siemens LOGO! 8 BM Devices)
    - Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method. This could allow an attacker to retrieve parts of the content of the memory.
- CVE-2022-36362: (Improper Input Validation Vulnerability in Siemens LOGO! 8 BM Devices)
    - Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device.
- CVE-2022-30790: (Buffer Overflow Vulnerability in Schneider EcoStruxure Panel Server Box)
    - An Out-of-Bounds Write vulnerability exists that could cause arbitrary writes when crafted malformed packets are received from a local network while U-boot is running
- CVE-2022-31766: (Denial of Service Vulnerability in the TCP Event Service of Siemens SCALANCE and RUGGEDCOM Products)
    - Affected devices with TCP Event service enabled do not properly handle malformed packets. This could allow an unauthenticated remote attacker to cause a denial of service condition and reboot the device thus possibly affecting other network resources.
- CVE-2022-30552: (Buffer Overflow Vulnerability in Schneider EcoStruxure Panel Server Box)
    - A Buffer Copy without Checking Size of Input vulnerability exists that could cause Denial of Service when a specially crafted fragmented IP Datagram with an invalid total length is received from a local network while U-boot is running.
- CVE-2022-36361: (Classic Buffer Overflow Vulnerability in Siemens LOGO! 8 BM Devices)
    - LOGO! 8 BM (incl. SIPLUS variants) contains multiple web-related vulnerabilities. These could allow an attacker to execute code remotely, put the device into a denial of service state or retrieve parts of the memory.
- CVE-2022-40226: (Access Control Vulnerability in the Web Server of Siemens SICAM P850 and SICAM P855 Devices)
    - Affected devices accept user defined session cookies and do not renew the session cookie after login/logout. This could allow an attacker to take over another user’s session after login.
- CVE-2022-20919: (Cisco IOS and IOS XE Software Common Industrial Protocol Request Denial of Service Vulnerability)
    - A vulnerability in the processing of malformed Common Industrial Protocol (CIP) packets that are sent to Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to unexpectedly reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation during processing of CIP packets. An attacker could exploit this vulnerability by sending a malformed CIP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to unexpectedly reload, resulting in a DoS condition. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

- CVE-2022-20920: (Cisco IOS and IOS XE Software SSH Denial of Service Vulnerability)
  - A vulnerability in the SSH implementation of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. This vulnerability is due to improper handling of resources during an exceptional situation. An attacker could exploit this vulnerability by continuously connecting to an affected device and sending specific SSH requests. A successful exploit could allow the attacker to cause the affected device to reload.
- CVE-2021-27862: (Vulnerabilities in Layer 2 Network Security Controls Affecting Cisco Products: September 2022)
  - On September 27, 2022, the following vulnerabilities affecting Cisco products were disclosed by Cert/CC as part of VU855201, titled L2 network security controls can be bypassed using VLAN 0 stacking and/or 802.3 headers:
    - CVE-2021-27853: Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using a combination of VLAN 0 headers and LLC/SNAP headers.
    - CVE-2021-27854: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using a combination of VLAN 0 headers, LLC/SNAP headers in Ethernet to Wifi frame translation, and in the reverse—Wifi to Ethernet.
    - CVE-2021-27861: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers).
    - CVE-2021-27862: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).

    Exploitation of these vulnerabilities could allow an adjacent attacker to bypass configured first-hop security (FHS) features on the affected Cisco products.
- CVE-2022-20849: (Cisco IOS XR Software Broadband Network Gateway PPP over Ethernet Denial of Service Vulnerability)
  - A vulnerability in the Broadband Network Gateway PPP over Ethernet (PPPoE) feature of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the PPPoE process to continually crash. This vulnerability exists because the PPPoE feature does not properly handle an error condition within a specific crafted packet sequence. An attacker could exploit this vulnerability by sending a sequence of specific PPPoE packets from controlled customer premises equipment (CPE). A successful exploit could allow the attacker to cause the PPPoE process to continually restart, resulting in a denial-of-service condition (DoS).
- CVE-2022-20856: (Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family CAPWAP Mobility Denial of Service Vulnerability)
  - A vulnerability in the processing of Control and Provisioning of Wireless Access Points (CAPWAP) Mobility messages in 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 a logic error and improper management of resources related to the handling of CAPWAP Mobility messages. An attacker could exploit this vulnerability by sending crafted CAPWAP Mobility packets to an affected device. A successful exploit could allow the attacker to exhaust resources on the affected device. This would cause the device to reload, resulting in a DoS condition.

- CVE-2022-20944: (Cisco IOS XE Software for Catalyst 9200 Series Switches Arbitrary Code Execution Vulnerability)
    - A vulnerability in the software image verification functionality of Cisco IOS XE Software for Cisco Catalyst 9200 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the boot process of the affected device. To exploit this vulnerability, the attacker needs either unauthenticated physical access to the device or privileged access to the root shell on the device. Note: In Cisco IOS XE Software releases 16.11.1 and later, root shell access is protected by the Consent Token mechanism. However, an attacker with level-15 privileges could easily downgrade the Cisco IOS XE Software running on a device to a release where root shell access is more readily available.
- CVE-2022-20915: (Cisco IOS XE Software IPv6 VPN over MPLS Denial of Service Vulnerability)
    - A vulnerability in the implementation of IPv6 VPN over MPLS (6VPE) with Zone-Based Firewall (ZBFW) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error handling of an IPv6 packet that is forwarded from an MPLS and ZBFW-enabled interface in a 6VPE deployment. An attacker could exploit this vulnerability by sending a crafted IPv6 packet sourced from a device on the IPv6-enabled virtual routing and forwarding (VRF) interface through the affected device. A successful exploit could allow the attacker to reload the device, resulting in a DoS condition.
- CVE-2022-20845: (Cisco Network Convergence System 4000 Series TL1 Denial of Service Vulnerability)
    - A vulnerability in the TL1 function of Cisco Network Convergence System (NCS) 4000 Series could allow an authenticated, local attacker to cause a memory leak in the TL1 process. This vulnerability is due to TL1 not freeing memory under some conditions. An attacker could exploit this vulnerability by connecting to the device and issuing TL1 commands after being authenticated. A successful exploit could allow the attacker to cause the TL1 process to consume large amounts of memory. When the memory reaches a threshold, the Resource Monitor (Resmon) process will begin to restart or shutdown the top five consumers of memory, resulting in a denial of service (DoS).
- CVE-2022-20855: (Cisco IOS XE Software for Embedded Wireless Controllers on Catalyst Access Points Privilege Escalation Vulnerability)
    - A vulnerability in the self-healing functionality of Cisco IOS XE Software for Embedded Wireless Controllers on Catalyst Access Points could allow an authenticated, local attacker to escape the

restricted controller shell and execute arbitrary commands on the underlying operating system of the access point. This vulnerability is due to improper checks throughout the restart of certain system processes. An attacker could exploit this vulnerability by logging on to an affected device and executing certain CLI commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root. To successfully exploit this vulnerability, an attacker would need valid credentials for a privilege level 15 user of the wireless controller.

- CVE-2022-20837: (Cisco IOS XE Software DNS NAT Protocol Application Layer Gateway Denial of Service Vulnerability)
  - A vulnerability in the DNS application layer gateway (ALG) functionality that is used by Network Address Translation (NAT) in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. This vulnerability is due to a logic error that occurs when an affected device inspects certain TCP DNS packets. An attacker could exploit this vulnerability by sending crafted DNS packets through the affected device that is performing NAT for DNS packets. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition on the affected device.
- CVE-2021-27861: (Vulnerabilities in Layer 2 Network Security Controls Affecting Cisco Products: September 2022)
  - On September 27, 2022, the following vulnerabilities affecting Cisco products were disclosed by Cert/CC as part of VU855201, titled L2 network security controls can be bypassed using VLAN 0 stacking and/or 802.3 headers:
    - CVE-2021-27853: Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using a combination of VLAN 0 headers and LLC/SNAP headers.
    - CVE-2021-27854: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using a combination of VLAN 0 headers, LLC/SNAP headers in Ethernet to Wifi frame translation, and in the reverse—Wifi to Ethernet.
    - CVE-2021-27861: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers).
    - CVE-2021-27862: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).

  Exploitation of these vulnerabilities could allow an adjacent attacker to bypass configured first-hop security (FHS) features on the affected Cisco products.
- CVE-2022-20824: (Cisco FXOS and NX-OS Software Cisco Discovery Protocol Denial of Service and Arbitrary Code Execution Vulnerability)
  - A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation of specific values that are within a Cisco Discovery Protocol

message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, which would cause the affected device to reload, resulting in a DoS condition.

- CVE-2022-20870: (Cisco IOS XE Software for Catalyst Switches MPLS Denial of Service Vulnerability)
    - A vulnerability in the egress MPLS packet processing function of Cisco IOS XE Software for Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 Family Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient input validation of IPv4 traffic. An attacker could exploit this vulnerability by sending a malformed packet out of an affected MPLS-enabled interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.
- CVE-2021-27853: (Vulnerabilities in Layer 2 Network Security Controls Affecting Cisco Products: September 2022)
    - On September 27, 2022, the following vulnerabilities affecting Cisco products were disclosed by Cert/CC as part of VU855201, titled L2 network security controls can be bypassed using VLAN 0 stacking and/or 802.3 headers:
        - CVE-2021-27853: Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using a combination of VLAN 0 headers and LLC/SNAP headers.
        - CVE-2021-27854: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using a combination of VLAN 0 headers, LLC/SNAP headers in Ethernet to Wifi frame translation, and in the reverse—Wifi to Ethernet.
        - CVE-2021-27861: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers).
        - CVE-2021-27862: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).
- CVE-2022-20810: (Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family SNMP Information Disclosure Vulnerability)
    - A vulnerability in the Simple Network Management Protocol (SNMP) of Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family could allow an authenticated, remote attacker to access sensitive information. This vulnerability is due to insufficient restrictions that allow a sensitive configuration detail to be disclosed. An attacker could exploit this vulnerability by retrieving data through SNMP read-only community access. A successful exploit could allow the attacker to view Service Set Identifier (SSID) preshared keys (PSKs) that are configured on the affected device.
- CVE-2022-20847: (Cisco IOS XE Wireless Controller Software for the Catalyst 9000 Family DHCP Processing

Denial of Service Vulnerability)

  - A vulnerability in the DHCP processing functionality 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. This vulnerability is due to the improper processing of DHCP messages. An attacker could exploit this vulnerability by sending malicious DHCP messages to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

- CVE-2022-20823: (Cisco NX-OS Software OSPFv3 Denial of Service Vulnerability)

  - A vulnerability in the OSPF version 3 (OSPFv3) 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 incomplete input validation of specific OSPFv3 packets. An attacker could exploit this vulnerability by sending a malicious OSPFv3 link-state advertisement (LSA) to an affected device. A successful exploit could allow the attacker to cause the OSPFv3 process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition. Note: The OSPFv3 feature is disabled by default. To exploit this vulnerability, an attacker must be able to establish a full OSPFv3 neighbor state with an affected device. For more information about exploitation conditions, see the Details section of this advisory.

- CVE-2022-20848: (Cisco IOS XE Software for Embedded Wireless Controllers on Catalyst 9100 Series Access Points UDP Processing Denial of Service Vulnerability)

  - A vulnerability in the UDP processing functionality of Cisco IOS XE Software for Embedded Wireless Controllers on Catalyst 9100 Series Access Points could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to the improper processing of UDP datagrams. An attacker could exploit this vulnerability by sending malicious UDP datagrams to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.

- CVE-2022-20851: (Cisco IOS XE Software Web UI Command 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 execute arbitrary commands on the underlying operating system with root privileges. To exploit this vulnerability, an attacker must have valid Administrator privileges on the affected device.

- CVE-2022-20846: (Cisco IOS XR Software Cisco Discovery Protocol Denial of Service Vulnerability)

  - A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the Cisco Discovery Protocol process to reload on an affected device. This vulnerability is due to a heap buffer overflow in certain Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a heap overflow, which could cause the Cisco Discovery Protocol process to reload on the device. The bytes that can be written in the buffer overflow are restricted, which limits remote code execution.

- CVE-2021-27854: (Vulnerabilities in Layer 2 Network Security Controls Affecting Cisco Products: September 2022)
    - On September 27, 2022, the following vulnerabilities affecting Cisco products were disclosed by Cert/CC as part of VU855201, titled L2 network security controls can be bypassed using VLAN 0 stacking and/or 802.3 headers:
        - CVE-2021-27853: Layer 2 network filtering capabilities such as IPv6 RA guard or ARP inspection can be bypassed using a combination of VLAN 0 headers and LLC/SNAP headers.
        - CVE-2021-27854: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using a combination of VLAN 0 headers, LLC/SNAP headers in Ethernet to Wifi frame translation, and in the reverse—Wifi to Ethernet.
        - CVE-2021-27861: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length (and optionally VLAN0 headers).
        - CVE-2021-27862: Layer 2 network filtering capabilities such as IPv6 RA guard can be bypassed using LLC/SNAP headers with invalid length and Ethernet to Wifi frame conversion (and optionally VLAN0 headers).

    Exploitation of these vulnerabilities could allow an adjacent attacker to bypass configured first-hop security (FHS) features on the affected Cisco products.

20221007

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

- **Talos Rules 2022-10-06 (https://www.snort.org/advisories/talos-rules-2022-10-06)**
    - Talos has added and modified multiple rules in the browser-webkit, file-other, os-mobile, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2022-10-04 (https://www.snort.org/advisories/talos-rules-2022-10-04)**
    - Talos has added and modified multiple rules in the browser-chrome, browser-other, file-identify, os-linux, os-mobile and server-webapp rule sets to provide coverage for emerging threats from these technologies.