Release Notes for Cisco Cyber Vision Knowledge DB

Release 202104

Compatible device list

Center	Description
All version 3 centers	All Cisco Cyber Vision center version 3 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-3.2.2.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-3.2.2.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-3.2.2.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-3.2.2.ext	Sensor Management extension installation file
Sensor	**Description**
CiscoCyberVision-IOx-aarch64-3.2.2.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3K-3.2.2.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-3.2.2.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-3.2.2.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-3.2.2.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates/3/3.2.2	**Description**
CiscoCyberVision-sysupgrade-3.2.2.dat	System Upgrade file for Center and Sensors 3.1.x to 3.2.2
CiscoCyberVision-sysupgrade-sensor-3.2.2.dat	Cisco Cyber Vision System Upgrade file for IC3000 Sensors or other non IOx Sensors 3.x to 3.2.2
CiscoCyberVision-Embedded-KDB-3.2.2.dat	Knowledge DB embedded in Cisco Cyber Vision 3.2.2
Updates/KDB/KDB.202104	**Description**
CiscoCyberVision_knowledgedb_20210402.db	Knowledge DB version 20210402
CiscoCyberVision_knowledgedb_20210409.db	Knowledge DB version 20210409
CiscoCyberVision_knowledgedb_20210416.db	Knowledge DB version 20210416
CiscoCyberVision_knowledgedb_20210423.db	Knowledge DB version 20210423
CiscoCyberVision_knowledgedb_20210430.db	Knowledge DB version 20210430

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_3_2_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

20210430

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

- **Talos Rules 2021-04-29 (https://www.snort.org/advisories/talos-rules-2021-04-29)**
  - Talos has added and modified multiple rules in the browser-ie, file-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-04-27 (https://www.snort.org/advisories/talos-rules-2021-04-27)**
  - Talos has added and modified multiple rules in the app-detect, browser-ie, browser-other, exploit-kit, file-pdf, malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

This release also adds support for the detection of the following vulnerability:

- CVE-2016-20009: (Stack-based overflow in the IPnet may lead to remote code execution (Name:Wreck))
  - In Wind River VxWorks versions 6.5 through 7, the DNS client (IPnet) has a stack-based overflow on the message decompression function. This may allow a remote, unauthenticated attacker to perform remote code execution.

20210423

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

- **Talos Rules 2021-04-22 (https://www.snort.org/advisories/talos-rules-2021-04-22)**
  - Talos has added and modified multiple rules in the and server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-04-21 (https://www.snort.org/advisories/talos-rules-2021-04-21)**
  - Talos has added and modified multiple rules in the browser-chrome, malware-cnc, policy-other, protocol-voip, server-apache and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-04-20 (https://www.snort.org/advisories/talos-rules-2021-04-20)**
  - 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.

20210416

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

- **Talos Rules 2021-04-15 (https://www.snort.org/advisories/talos-rules-2021-04-15)**
  - Talos has added and modified multiple rules in the browser-chrome, file-pdf, indicator-obfuscation, malware-backdoor, malware-cnc and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-04-13 (https://www.snort.org/advisories/talos-rules-2021-04-13)**

- Talos Microsoft Vulnerability CVE-2021-28310: 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 57403 through 57404.
- Microsoft Vulnerability CVE-2021-28324: A coding deficiency exists in Microsoft SMB that may lead to information disclosure.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 57411.
- Microsoft Vulnerability CVE-2021-28325: A coding deficiency exists in Microsoft SMB that may lead to information disclosure.
    - A rule to detect attacks targeting this vulnerability is included in this release and is identified with GID 1, SID 57414.
- Talos also has added and modified multiple rules in the malware-cnc, os-windows 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-2021-25667: (Stack-based Buffer Overflow in Siemens SCALANCE and RUGGEDCOM Devices)
    - Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution. Successful exploitation requires the passive listening feature of the device to be active.
- CVE-2019-6572: (Multiple Vulnerabilities in SIMATIC Panels and SIMATIC WinCC (TIA Portal))
    - A vulnerability has been identified in SIMATIC HMI Comfort Panels 4" - 22" (All versions < V15.1 Update 1), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V15.1 Update 1), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 und KTP900F (All versions < V15.1 Update 1), SIMATIC WinCC Runtime Advanced (All versions < V15.1 Update 1), SIMATIC WinCC Runtime Professional (All versions < V15.1 Update 1), SIMATIC WinCC (TIA Portal) (All versions < V15.1 Update 1), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). The affected device offered SNMP read and write capacities with a publicly know hardcoded community string. The security vulnerability could be exploited by an attacker with network access to the affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity of the affected system. At the time of advisory publication, no public exploitation of this security vulnerability was known.
- CVE-2019-11478: (Uncontrolled Resource Consumption Vulnerability in multiple Siemens Industrial Products)
    - Successful exploitation of these vulnerabilities could cause denial-of-service condition.
- CVE-2019-11477: (Integer Overflow Or Wraparound Vulnerability in multiple Siemens Industrial Products)
    - Successful exploitation of these vulnerabilities could cause denial-of-service condition.
- CVE-2015-8214: (Authentication Bypass Vulnerability in SIMATIC NET CP Modules and TIM Devices)
    - The implemented access protection level enforcement of the affected communication processors (CP)could possibly allow unauthenticated users to perform administrative operations on the CPs if network access (port 102/TCP) is available and the CPs' configuration was stored on their corresponding CPUs.

- CVE-2019-11479: (Uncontrolled Resource Consumption Vulnerability in multiple Siemens Industrial Products)
    - Successful exploitation of these vulnerabilities could cause denial-of-service condition.
- CVE-2018-18065: (Denial-of-Service Vulnerability over SNMP in Multiple Industrial Products)
    - A NULL Pointer Exception bug within the SMNP handling code allows authenticated attacker to remotely cause a Denial-of-Service (DoS) via a crafted packet sent on port 161/udp (SNMP).The security vulnerability could be exploited by an attacker with network access to the affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the affected system.
- CVE-2015-5621: (Denial-of-Service Vulnerability over SNMP in Multiple Industrial Products)
    - An error in the message handling of SNMP messages allows remote attackers to cause a Denial-of-Service (DoS) and possibly execute arbitrary code via a crafted packet sent on port 161/udp (SNMP). The security vulnerability could be exploited by an attacker with network access to the affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the affected system.
- CVE-2019-6585: (Cross-Site Scripting Vulnerability in Siemens SCALANCE S-600)
    - These vulnerabilities could allow a remote attacker to conduct denial-of-service or cross-site scripting attacks. User interaction is required for a successful exploitation of the cross-site-scripting attack.
- CVE-2019-13926: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE S-600)
    - These vulnerabilities could allow a remote attacker to conduct denial-of-service or cross-site scripting attacks. User interaction is required for a successful exploitation of the cross-site-scripting attack.
- CVE-2019-13925: (Uncontrolled Resource Consumption Vulnerability in Siemens SCALANCE S-600)
    - These vulnerabilities could allow a remote attacker to conduct denial-of-service or cross-site scripting attacks. User interaction is required for a successful exploitation of the cross-site-scripting attack.
- CVE-2019-13924: (Protection Mechanism Failure Vulnerability in Siemens SCALANCE X Switches)
    - The device does not send the X-Frame-Option Header in the administrative web interface, which makes it vulnerable to Clickjacking attacks. The security vulnerability could be exploited by an attacker that is able to trick an administrative user with a valid session on the target device into clicking on a website controlled by the attacker. The vulnerability could allow an attacker to perform administrative actions via the web interface
- CVE-2019-8460: (Excessive Data Query Operations in a Large Data Table in Siemens Industrial Products)
    - OpenBSD kernel version <= 6.5 can be forced to create long chains of TCP SACK holes that causes very expensive calls to tcp_sack_option() for every incoming SACK packet which can lead to a denial of service.
- 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-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-2021-25667: (Stack-based Buffer Overflow in Siemens SCALANCE and RUGGEDCOM Devices)
    - Affected devices contain a stack-based buffer overflow vulnerability in the handling of STP BPDU frames that could allow a remote attacker to trigger a denial-of-service condition or potentially remote code execution. Successful exploitation requires the passive listening feature of the device to be active
- CVE-2021-25676: (Improper Restriction of Excessive Authentication Attempts in Siemens SCALANCE and RUGGEDCOM Devices)
    - Multiple failed SSH authentication attempts could trigger a temporary Denial-of-Service under certain conditions. When triggered, the device will reboot automatically
- CVE-2015-5219: (Incorrect Type Conversion or Cast in ntpd)
    - The ULOGTOD function in ntp.d in SNTP before 4.2.7p366 does not properly perform type conversions from a precision value to a double, which allows remote attackers to cause a denial of service (infinite loop) via a crafted NTP packet.
- CVE-2016-4953: (Improper Authentication in ntpd)
    - ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (ephemeral-association demobilization) by sending a spoofed crypto-NAK packet with incorrect authentication data at a certain time.
- CVE-2015-7974: (Improper Authentication in ntpd)
    - NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a “skeleton key.
- CVE-2016-1547: (Improper Input Validation in ntpd)
    - An off-path attacker can cause a preemptible client association to be demobilized in NTP 4.2.8p4 and earlier and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled.
- CVE-2020-27737: (Out-of-bounds Read in the DNS Module of Nucleus Products)
    - The DNS response parsing functionality does not properly validate various length and counts of the records. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the memory past the allocated structure.
- CVE-2015-7705: (Improper Input Validation in ntpd)
    - The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified impact via a large number of crafted requests
- CVE-2015-7855: (Improper Input Validation in ntpd)
    - The decodenetnum function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (assertion failure) via a 6 or mode 7 packet containing a long data value.
- CVE-2015-8138: (Improper Input Validation in ntpd)

    - NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to bypass the origin timestamp validation via a packet with an origin timestamp set to zero.
- CVE-2015-7871: (Improper Authentication in ntpd)
    - Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.
- CVE-2021-25669: (Stack-based Buffer Overflow in Siemens Web Server of SCALANCE X200)
    - Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution
- CVE-2021-1352: (Cisco IOS XE Software DECnet Phase IV/OSI Denial of Service Vulnerability)
    - A vulnerability in the DECnet Phase IV and DECnet/OSI protocol processing of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation of DECnet traffic that is received by an affected device. An attacker could exploit this vulnerability by sending DECnet traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-decnet-dos-cuPWDkyL
- CVE-2021-1452: (Cisco IOS XE ROM Monitor Software for Cisco Industrial Switches OS Command Injection Vulnerability)
    - A vulnerability in the ROM Monitor (ROMMON) of Cisco IOS XE Software for Cisco Catalyst IE3200, IE3300, and IE3400 Rugged Series Switches, Cisco Catalyst IE3400 Heavy Duty Series Switches, and Cisco Embedded Services 3300 Series Switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. This vulnerability is due to incorrect validations of specific function arguments passed to a boot script when specific ROMMON variables are set. An attacker could exploit this vulnerability by setting malicious values for a specific ROMMON variable. A successful exploit could allow the attacker to execute unsigned code and bypass the image verification check during the secure boot process of an affected device. To exploit this vulnerability, the attacker would need to have unauthenticated, physical access to the device or obtain privileged access to the root shell on the device. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-romvar-cmd-inj-N56fYbrw
- CVE-2015-7977: (NULL Pointer Dereference in ntpd)
    - ntpd in NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial ofservice (NULL pointer dereference) via a ntpdc reslist command.
- CVE-2021-25677: (Use of Insufficiently Random Values in the DNS Module of Nucleus Products)
    - The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.
- CVE-2016-1548: (Data Processing Errors in ntpd)
    - An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client in NTP 4.2.8p4 and earlier

and NTPSec aa48d001683e5b791a743ec9c575aaf7d867a2b0c will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has beenchanged. ntpq gives no indication that the mode has been switched.

- CVE-2016-4954: (Race Condition in ntpd)
  - The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many sourceIP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication.
- CVE-2015-7973: (Security Features in ntpd)
  - NTP before 4.2.8p6 and 4.3.x before 4.3.90, when configured in broadcast mode, allows man-in-the-middle attackers to conduct replay attacks by sniffing the network.
- CVE-2015-7979: (Data Processing Errors in ntpd)
  - NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service(client-server association tear down) by sending broadcast packets with invalid authentication to a broadcast client.
- CVE-2020-27736: (Improper Null Termination in the DNS Module of Nucleus Products)
  - The DNS domain name label parsing functionality does not properly validate the null-terminated name in DNS-responses. The parsing of malformed responses could result in a read past the end of an allocated structure. An attacker with a privileged position in the network could leverage this vulnerability to cause a denial-of-service condition or leak the read memory.
- CVE-2021-25668: (Heap-based Buffer Overflow in Siemens Web Server of SCALANCE X200)
  - Incorrect processing of POST requests in the web server may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.
- CVE-2016-1550: (Exposure of Sensitive Information to an Unauthorized Actor in ntpd)
  - An exploitable vulnerability exists in the message authentication functionality of libntp in ntp 4.2.8p4 and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92. An attacker can send a series of crafted messages to attempt to recover the message digest key.

20210409

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

- **Talos Rules 2021-04-08 (https://www.snort.org/advisories/talos-rules-2021-04-08)**
  - Talos has added and modified multiple rules in the browser-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

20210402

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

- **Talos Rules 2021-04-01 (https://www.snort.org/advisories/talos-rules-2021-04-01)**
  - Talos has added and modified multiple rules in the browser-ie, exploit-kit, indicator-obfuscation, indicator-shellcode, malware-cnc, netbios, protocol-dns, protocol-voip, server-oracle and server-webapp rule sets to provide coverage for emerging threats from these technologies.

- **Talos Rules 2021-03-30 (https://www.snort.org/advisories/talos-rules-2021-03-30)**
  - Talos has added and modified multiple rules in the browser-other, malware-cnc, os-windows, protocol-tftp and server-webapp rule sets to provide coverage for emerging threats from these technologies.