# Release Notes for Cisco Cyber Vision Knowledge DB

# Release 202111

# 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-4.0.2.ova** | VMWare OVA file, for Center setup |
| **CiscoCyberVision-center-4.0.2.vhdx** | Hyper-V VHDX file, for Center setup |
| **CiscoCyberVision-center-with-DPI-4.0.2.ova** | VMWare OVA file, for Center with DPI setup |
| **CiscoCyberVision-sensor-management-4.0.2.ext** | Sensor Management extension installation file |
| **Sensor** | **Description** |
| **CiscoCyberVision-IOx-aarch64-4.0.2.tar** | Cisco IE3400 and Cisco IR1101 installation and update file |
| **CiscoCyberVision-IOx-IC3K-4.0.2.tar** | Cisco IC3000 sensor installation and update file |
| **CiscoCyberVision-IOx-x86-64-4.0.2.tar** | Cisco Catalyst 9300 installation and update file |
| **CiscoCyberVision-IOx-Active-Discovery-aarch64-4.0.2.tar** | Cisco IE3400 installation and update file, for Sensor with Active Discovery |
| **CiscoCyberVision-IOx-Active-Discovery-x86-64-4.0.2.tar** | Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery |
| **Updates/4/4.0.2** | **Description** |
| **CiscoCyberVision-Embedded-KDB-4.0.2.dat** | Knowledge DB embedded in Cisco Cyber Vision 4.0.2 |
| **Updates/KDB/KDB.202111** | **Description** |
| **CiscoCyberVision_knowledgedb_20211105.db** | Knowledge DB version 20211105 |
| **CiscoCyberVision_knowledgedb_20211115.db** | Knowledge DB version 20211115 |
| **CiscoCyberVision_knowledgedb_20211119.db** | Knowledge DB version 20211119 |
| **CiscoCyberVision_knowledgedb_20211126.db** | Knowledge DB version 20211126 |

## 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

## 20211126

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

- **Talos Rules 2021-11-25 (https://www.snort.org/advisories/talos-rules-2021-11-25)**
  - Microsoft Vulnerability CVE-2021-42321: A remote code execution vulnerability exists in Microsoft Exchange Server for which exploit code is publicly available.
  - Rules to detect attacks targeting this vulnerability are included in this release and are identified with GID 1, SIDs 58637 through 58639.
  - Talos has added and modified multiple rules in the server-other rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-11-23 (https://www.snort.org/advisories/talos-rules-2021-11-23)**
  - In this release a number of rules have been added to the security policy as part of ongoing policy rebalancing efforts.
  - Microsoft Vulnerability CVE-2021-41379: A coding deficiency exists in Microsoft Windows Installer that may lead to an escalation of privilege.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58635 through 58636.
  - Talos also has added and modified multiple rules in the browser-chrome, browser-firefox, browser-plugins, file-java, file-other, netbios, os-mobile, os-other, os-solaris, os-windows, policy-other, protocol-imap, protocol-nntp, protocol-pop, protocol-rpc, protocol-scada, protocol-services, protocol-snmp, server-apache, server-iis, server-mysql, server-oracle, server-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.

## 20211119

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

- **Talos Rules 2021-11-18 (https://www.snort.org/advisories/talos-rules-2021-11-18)**
  - In this release a number of rules have been added to the security policy as part of ongoing policy rebalancing efforts.
  - Talos has added and modified multiple rules in the browser-chrome, browser-firefox, browser-ie, browser-other, browser-plugins, browser-webkit, exploit-kit, file-flash, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, malware-cnc, malware-tools, netbios, os-linux, os-mobile, os-windows, policy-other, protocol-dns, protocol-icmp, pua-other, server-apache, server-iis, server-mail, server-oracle and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-11-16 (https://www.snort.org/advisories/talos-rules-2021-11-16)**
  - Talos has added and modified multiple rules in the exploit-kit, file-image, file-multimedia, file-other, malware-cnc, netbios, os-mobile, os-solaris, policy-other, protocol-imap, server-mysql and server-webapp rule sets to provide coverage for emerging threats from these technologies.

## 20211115

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

- **Talos Rules 2021-11-10 (https://www.snort.org/advisories/talos-rules-2021-11-10)**
  - Talos has added and modified multiple rules in the browser-ie and server-webapp rule sets to provide coverage for emerging threats from these technologies
- **Talos Rules 2021-11-09 (https://www.snort.org/advisories/talos-rules-2021-11-09)**
  - Microsoft Vulnerability CVE-2021-38666: A coding deficiency exists in Remote Desktop Client 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 58541.
  - Microsoft Vulnerability CVE-2021-42292: A coding deficiency exists in Microsoft Excel that may lead to security feature bypass.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58539 through 58540, or GID 1 SID 300054 for Snort3.
  - Microsoft Vulnerability CVE-2021-42298: A coding deficiency exists in Microsoft Defender that may lead to remote code execution.
  - Rules to detect attacks targeting these vulnerabilities are included in this release and are identified with GID 1, SIDs 58519 through 58520.
  - Talos also has added and modified multiple rules in the browser-ie, file-image, file-office, file-other, malware-cnc, os-windows, server-mail 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-2021-34598: (Allocation of Resources Without Limits or Throttling in Phoenix Contact FL MGUARD 1102/1105)
  The remote logging functionality is impaired by the lack of memory release for data structures from syslog-ng when remote logging is active (CWE-770: Allocation of Resources Without Limits or Throttling).
- CVE-2021-34582: (Improper Neutralization of Input During Web Page Generation in Phoenix Contact FL MGUARD 1102/1105)
  The file upload functionality in the web-based management is affected by a stored cross-site scripting vulnerability (CWE-79: Improper Neutralization of Input During Web Page Generation). An authenticated FL MGUARD user with Admin or Super Admin role can upload a certificate file on the Basic settings > LDAP page, on the Logs > Remote logging page, or through the REST API. The content of this file is embedded into the corresponding web page, and any HTML code within the file is rendered when the page is viewed by the same or a different authenticated user.
- CVE-2020-28895: (Integer Overflow or Wraparound and Out-of-bounds Write in Wind River VxWorks)
  In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.
- CVE-2020-35198: (Integer Overflow or Wraparound in Wind River VxWorks 7)
  An issue was discovered in Wind River VxWorks 7. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by calloc(). As a result, the actual memory allocated is

smaller than the buffer size specified by the arguments, leading to memory corruption.

- CVE-2021-22156: (Integer Overflow or Wraparound in BlackBerry QNX)
  An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code.
- CVE-2021-22816: (Improper Check for Unusual or Exceptional Conditions vulnerability in Schneider Electric SCADAPack 300E Series RTU)
  A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a Denial of Service of the RTU when receiving a specially crafted request over Modbus, and the RTU is configured as a Modbus server.
- CVE-2021-22815: (Information Exposure in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-200: Information Exposure vulnerability exists which could cause the troubleshooting archive to be accessed.
- CVE-2021-22813: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to an edit policy file.
- CVE-2021-22812: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC.
- CVE-2021-22810: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause arbitrary script execution when a privileged account clicks on a malicious URL specifically crafted for the NMC pointing to a delete policy file.
- CVE-2021-22811: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause script execution when the request of a privileged account accessing the vulnerable web page is intercepted.
- CVE-2021-22814: (Cross-site Scripting in Schneider Electric Network Management Cards (NMC) and NMC Embedded Devices)
  A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists which could cause arbitrary script execution when a malicious file is read and displayed.
- CVE-2021-37732: ( Command Injection Vulnerability in Siemens SCALANCE W1750D)
  A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) web-based management user interface. Successful exploitation could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the system.
- CVE-2021-31345: ( Improper Validation of Specified Quantity in Input Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)

The total length of an UDP payload (set in the IP header) is unchecked. This may lead to various side effects, including information leaks, depending on a user-defined application that runs on top of the UDP protocol.

- CVE-2021-31887: ( Improper Null Termination Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  FTP server does not properly validate the length of the “PWD/XPWD” command, leading to stack-based buffer overflows. This may result in denial-of-service conditions and remote code execution.
- CVE-2021-40366: (Missing Encryption of Sensitive Data Vulnerability in Siemens Climatix POL909 (AWM module))
  The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.
- CVE-2021-31885: ( Buffer Access with Incorrect Length Value Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  TFTP server application allows for reading the contents of the TFTP memory buffer via sending malformed TFTP commands.
- CVE-2021-31888: (Improper Null Termination Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  FTP server does not properly validate the length of the “MKD/XMKD” command, leading to stack-based buffer overflows. This may result in denial-of-service conditions and remote code execution.
- CVE-2021-37726: (Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability in Siemens SCALANCE W1750D)
  A remote buffer overflow vulnerability was discovered in HPE Aruba Instant (IAP). Successful exploitation could allow for unauthenticated remote code execution, potentially resulting in the execution of arbitrary code as a privileged user on the underlying system.
- CVE-2021-31881: ( Out-of-bounds Read Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to denial-of-service conditions.
- CVE-2021-31883: ( Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to denial-of-service conditions.
- CVE-2021-31886: (Improper Null Termination Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  FTP server does not properly validate the length of the “USER” command, leading to stack-based buffer overflows. This may result in denial-of-service conditions and remote code execution.
- CVE-2021-37734: ( Path Traversal Vulnerability in Siemens SCALANCE W1750D)
  An authenticated arbitrary file read access vulnerability was discovered in Aruba Instant Access Points. Successful exploitation could lead to an attacker reading any file off the underlying filesystem, including system sensitive files.
- CVE-2021-31346: ( Improper Validation of Specified Quantity in Input Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including information leaks and denial-of-service conditions, depending on the network buffer organization in memory.

- CVE-2021-31889: ( Integer Underflow Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  Malformed TCP packets with a corrupted SACK option leads to denial-of-service conditions.
- CVE-2021-31884: ( Improper Null Termination Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  The DHCP client application assumes the data supplied with the "Hostname" DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to out-of-bound reads, writes, and denial-of-service conditions.
- CVE-2021-37735: ( Path Traversal Vulnerability in Siemens SCALANCE W1750D)
  A remote denial of service vulnerability was discovered in Aruba Instant through the command line interface. Successful exploitation could create a denial-of-service condition, leading to a temporary loss of service until the next reboot.
- CVE-2021-31344: (Type Confusion Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network.
- CVE-2021-31882: ( Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to denial-of-service conditions.
- CVE-2021-37730: ( Command Injection Vulnerability in Siemens SCALANCE W1750D)
  A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) command line interface. Successful exploitation could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the system.
- CVE-2021-31890: ( Improper Handling of Inconsistent Structural Elements Vulnerability in Siemens Nucleus RTOS based APOGEE and TALON Products)
  The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including denial-of-service conditions, depending on the network buffer organization in memory.
- CVE-2021-37727: ( Command Injection Vulnerability in Siemens SCALANCE W1750D)
  A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) command line interface. Successful exploitation could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the system.

## 20211105

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

- **Talos Rules 2021-11-04 (https://www.snort.org/advisories/talos-rules-2021-11-04)**
  - Talos has added and modified multiple rules in the browser-chrome, malware-cnc, malware-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.
- **Talos Rules 2021-11-02 (https://www.snort.org/advisories/talos-rules-2021-11-02)**
  - Talos has added and modified multiple rules in the malware-cnc, malware-other, policy-other and server-webapp rule sets to provide coverage for emerging threats from these technologies.