



# Release Notes for Cisco Cyber Vision Knowledge DB

## Release 202601

<b>Compatible device list</b> .....	<b>2</b>
<b>Links</b> .....	<b>2</b>
<b>Software Download</b> .....	<b>2</b>
<b>Related Documentation</b> .....	<b>3</b>
<b>Database download</b> .....	<b>3</b>
<b>How to update the database</b> .....	<b>3</b>
<b>Release contents</b> .....	<b>4</b>
<b>20260130</b> .....	<b>4</b>
Snort rules .....	4
Vulnerabilities .....	4
Vendor Database .....	6
<b>20260123</b> .....	<b>6</b>
Snort rules .....	6
Vulnerabilities .....	7
<b>20260116</b> .....	<b>18</b>
Snort rules .....	18
Vulnerabilities .....	19
<b>20260109</b> .....	<b>19</b>
Snort rules .....	20

## Compatible device list

Center	Description
All version 4 and 5 centers	All Cisco Cyber Vision center version 4 and 5 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-5.3.3.ova	VMWare OVA file, for Center setup
CiscoCyberVision-center-5.3.3.vhdx	Hyper-V VHDX file, for Center setup
CiscoCyberVision-center-with-DPI-5.3.3.ova	VMWare OVA file, for Center with DPI setup
CiscoCyberVision-sensor-management-5.3.3.ext	Sensor Management extension installation file
Sensor	Description
CiscoCyberVision-IOx-aarch64-5.3.3.tar	Cisco IE3400 and Cisco IR1101 installation and update file
CiscoCyberVision-IOx-IC3000-5.3.3.tar	Cisco IC3000 sensor installation and update file
CiscoCyberVision-IOx-x86-64-5.3.3.tar	Cisco Catalyst 9300 installation and update file
CiscoCyberVision-IOx-Active-Discovery-aarch64-5.3.3.tar	Cisco IE3400 installation and update file, for Sensor with Active Discovery
CiscoCyberVision-IOx-Active-Discovery-x86-64-5.3.3.tar	Cisco Catalyst 9300 installation and update file, for Sensor with Active Discovery
Updates	Description
CiscoCyberVision-Embedded-KDB-5.3.3.dat	Knowledge DB embedded in Cisco Cyber Vision 5.3.3
Updates/KDB/KDB.202601	Description
CiscoCyberVision_knowledgedb_20260109.db	Knowledge DB version 20260109
CiscoCyberVision_knowledgedb_20260116.db	Knowledge DB version 20260116
CiscoCyberVision_knowledgedb_20260123.db	Knowledge DB version 20260123
CiscoCyberVision_knowledgedb_20260130.db	Knowledge DB version 20260130

## 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](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

### 20260130

#### Snort rules

This release includes additions and modifications to the Snort ruleset covering the following Talos advisory:

- **Talos Rules 2026-01-29** (<https://www.snort.org/advisories/talos-rules-2026-01-29>)
- **Talos Rules 2026-01-27** (<https://www.snort.org/advisories/talos-rules-2026-01-27>)

The new and updated Snort rules span the following categories:

- 6 file-multimedia rules with SIDs 65794, 65790, 65792, 65789, 65791, 65793
- 4 file-office rules with SIDs 301386, 301387, 301385, 301384
- 1 file-pdf rules with SID 301383
- 1 policy-other rule with SID 65822
- 1 protocol-other rule with SID 65808
- 1 protocol-telnet rule with SID 65762
- 64 server-webapp rules with SIDs 62648, 65821, 65780, 65760, 65770, 57835, 65765, 65782, 65802, 65769, 65758, 65766, 65798, 65771, 65775, 65781, 65768, 65764, 65799, 301381, 65803, 65777, 59334, 65761, 65801, 65753, 65797, 65759, 65767, 58065, 65804, 65806, 65763, 65755, 59333, 301382, 65807, 65776, 65805, 65772, 65785, 65757, 65786, 65774, 65773, 58066, 57836, 65800, 65754, 65756, 65815, 65809, 65816, 65820, 65818, 65819, 65810, 65817, 65811, 65812, 65813, 65784, 65783, 65814

#### Vulnerabilities

This release adds support for the detection of vulnerabilities on Festo and Inductive Automation products:

- CVE-2025-11743: Denial-of-Service Vulnerability in Rockwell Automation CompactLogix 5370
  - A denial-of-service security issue in the affected product. The security issue occurs when a malformed CIP forward open message is sent. This could result in a major nonrecoverable fault and a restart is required to recover.
- CVE-2025-13823: Denial-of-Service Vulnerability in Rockwell Automation Micro850 and Micro870 Controllers
  - A security issue was found in the IPv6 stack in the Micro850 and Micro870 controllers when the controllers received multiple malformed packets during fuzzing. The controllers will go into recoverable fault with fault code 0xFE60. To recover the controller, clear the fault.
- CVE-2025-13824: Denial-of-Service Vulnerability in Rockwell Automation Micro800 Controllers

- A security issue exists due to improper handling of malformed CIP packets during fuzzing. The controller enters a hard fault with solid red Fault LED and becomes unresponsive. Upon power cycle, the controller will enter recoverable fault where the MS LED and Fault LED become flashing red and reports fault code 0xF019. To recover, clear the fault.
- CVE-2025-9278: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. After running a Burp Suite active scan, the device loses ICMP connectivity, causing the web application to become inaccessible.
- CVE-2025-9279: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP Step Limit Storm tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2025-9280: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. Fuzzing performed using Defensics causes the device to become unresponsive, requiring a reboot.
- CVE-2025-9281: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive step limit storm tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2025-9282: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive limited storm tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2025-9283: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP Step Limits Storms tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2025-9464: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. This vulnerability is triggered during fuzzing of multiple CIP classes, which causes the CIP port to become unresponsive.
- CVE-2025-9465: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT
  - A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles Comprehensive grammar tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2025-9466: Denial-of-Service Vulnerability in Rockwell Automation ArmorStart LT

- A security issue exists within ArmorStart® LT that can result in a denial-of-service condition. During execution of the Achilles EtherNet/IP and CIP grammar tests, the device reboots unexpectedly, causing the Link State Monitor to go down for several seconds.
- CVE-2019-16748: Remote Code Execution Vulnerability in Rockwell Automation PanelView 800
  - In WolfSSL through version 4.1.0, there is a missing sanity check of memory accesses in parsing ASN.1 certificate data while handshaking. There is a one-byte heap-based buffer over-read in CheckCertSignature in wolfcrypt/src/asn.c. WolfSSL is utilized in the PanelView 800. This could allow an attacker to accomplish a heap buffer overflow if the user has the email feature enabled in the project file where WolfSSL is used. This feature is disabled by default.
- CVE-2020-36177: Remote Code Execution Vulnerability in Rockwell Automation PanelView 800
  - RsaPad\_PSS in WolfSSL before version 4.6.0 has an out-of-bounds write. It is utilized in the PanelView 800 and could allow an attacker to accomplish a heap buffer overflow. This happens if the user has the email feature enabled in the project file where WolfSSL is used. The feature is disabled by default.

## Vendor Database

The new UI in Cyber Vision relies on a vendor database included in this Knowledge Base to represent physical assets and give them a type. This release adds initial typing support for assets from GE Vernova. It also improves support for assets from SEL.

## 20260123

### Snort rules

This release includes additions and modifications to the Snort ruleset covering the following Talos advisory:

- **Talos Rules 2026-01-22** (<https://www.snort.org/advisories/talos-rules-2026-01-22>)
- **Talos Rules 2026-01-20** (<https://www.snort.org/advisories/talos-rules-2026-01-20>)

The new and updated Snort rules span the following categories:

- 6 browser-ie rules with SIDs 63981, 63982, 65704, 65705, 63980, 65703
- 4 file-multimedia rules with SIDs 65741, 65742, 65739, 65738
- 7 malware-cnc rules with SIDs 65706, 65729, 65727, 65707, 65726, 65728, 65746
- 4 malware-other rules with SIDs 301380, 301376, 301378, 301377
- 1 policy-other rule with SID 65733
- 1 server-other rule with SID 65740

- 34 server-webapp rules with SIDs 65732, 65720, 65719, 65718, 65717, 65725, 65747, 46526, 301379, 46524, 65700, 65721, 65722, 65737, 65734, 65702, 65699, 65714, 43822, 65749, 65724, 65745, 65736, 59016, 65744, 43824, 65735, 65743, 65748, 65723, 65701, 65750, 65752, 65751

## Vulnerabilities

This release adds support for the detection of vulnerabilities on Festo and Inductive Automation products:

- CVE-2010-5250: Untrusted Search Path vulnerability for Festo Controller CECC-S,-LK,-D
  - Untrusted search path vulnerability in the pthread\_win32\_process\_attach\_np function in pthreadGC2.dll in Pthreads-win32 2.8.0 allows local users to gain privileges via a Trojan horse quserex.dll file in the current working directory
- CVE-2018-0739: Uncontrolled Recursion vulnerability for Festo Controller CECC-S,-LK,-D
  - Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
- CVE-2018-10612: Missing Encryption of Sensitive Data vulnerability for Festo Controller CECC-S,-LK,-D
  - In 3S-Smart Software Solutions GmbH CODESYS Control V3 products prior to version 3.5.14.0, user access management and communication encryption is not enabled by default, which could allow an attacker access to the device and sensitive information, including user credentials.
- CVE-2018-20025: Use of Insufficiently Random Values vulnerability for Festo Controller CECC-S,-LK,-D
  - Use of Insufficiently Random Values exists in CODESYS V3
- CVE-2018-20026: Improper Restriction of Communication Channel to Intended Endpoints vulnerability for Festo Controller CECC-S,-LK,-D
  - Improper Communication Address Filtering exists in CODESYS V3 products versions prior V3.5.14.0.
- CVE-2019-13532: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability for Festo Controller CECC-S,-LK,-D
  - CODESYS V3 web server, all versions prior to 3.5.14.10, allows an attacker to send specially crafted http or https requests which may allow access to files outside the restricted working directory of the controller.
- CVE-2019-13542: NULL Pointer Dereference vulnerability for Festo Controller CECC-S,-LK,-D
  - CODESYS V3 OPC UA Server, all versions 3.5.11.0 to 3.5.15.0, allows an attacker to send crafted requests from a trusted OPC UA client that cause a NULL pointer dereference, which may trigger a denial-of-service condition.
- CVE-2019-13548: Out-of-bounds Write vulnerability for Festo Controller CECC-S,-LK,-D

- CODESYS V3 web server, all versions prior to 3.5.14.10, allows an attacker to send specially crafted http or https requests which could cause a stack overflow and create a denial-of-service condition or allow remote code execution.
- CVE-2019-18858: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability for Festo Controller CECC-S,-LK,-D
  - CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.
- CVE-2019-5105: Out-of-bounds Write vulnerability for Festo Controller CECC-S,-LK,-D
  - An exploitable memory corruption vulnerability exists in the Name Service Client functionality of 3S-Smart Software Solutions CODESYS GatewayService. A specially crafted packet can cause a large memcpy, resulting in an access violation and termination of the process.
- CVE-2019-9010: Unverified Ownership vulnerability for Festo Controller CECC-S,-LK,-D
  - The CODESYS Gateway does not correctly verify the ownership of a communication channel.
- CVE-2019-9012: Allocation of Resources Without Limits or Throttling vulnerability for Festo Controller CECC-S,-LK,-D
  - A crafted communication request may cause uncontrolled memory allocations in the affected CODESYS products and may result in a denial-of-service condition.
- CVE-2019-9013: Use of a Broken or Risky Cryptographic Algorithm vulnerability for Festo Controller CECC-S,-LK,-D
  - An issue was discovered in 3S-Smart CODESYS V3 products. The application may utilize non-TLS based encryption, which results in user credentials being insufficiently protected during transport.
- CVE-2020-10644: Deserialization RCE in Inductive Automation Ignition
  - The affected product lacks proper validation of user-supplied data, which can result in deserialization of untrusted data on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information.
- CVE-2020-12000: Deserialization of Untrusted Data in Inductive Automation Ignition
  - The affected product is vulnerable to the handling of serialized data. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data.
- CVE-2020-12004: Information Disclosure in Inductive Automation Ignition
  - The affected product lacks proper authentication required to query the server on the Ignition 8 Gateway (versions prior to 8.0.10) and Ignition 7 Gateway (versions prior to 7.9.14), allowing an attacker to obtain sensitive information.
- CVE-2020-12067: Weak Password Recovery Mechanism for Forgotten Password vulnerability for Festo Controller CECC-S,-LK,-D
  - The user password can be changed without having to enter the original password.
- CVE-2020-12068: Improper Privilege Management vulnerability for Festo Controller CECC-S,-LK,-D

- An issue was discovered in CODESYS Development System before 3.5.16.0. CODESYS WebVisu and CODESYS Remote TargetVisu are susceptible to privilege escalation.
- CVE-2020-12069: Use of Password Hash With Insufficient Computational Effort Vulnerability for Festo Controller CECC-S,-LK,-D
  - In CODESYS V3 products in all versions prior V3.5.16.0 containing the CmpUserMgr, the CODESYS Control runtime system stores the online communication passwords using a weak hashing algorithm. This can be used by a local attacker with low privileges to gain full control of the device.
- CVE-2020-14479: Missing Authentication for Critical Function in Inductive Automation Ignition
  - Sensitive information can be obtained through the handling of serialized data. The issue results from the lack of proper authentication required to query the server
- CVE-2020-14520: Missing Authorization in Inductive Automation Ignition
  - The affected product is vulnerable to an information leak, which may allow an attacker to obtain sensitive information. An HTTP request to the unprotected API could be used to determine whether an arbitrary file path exists on the filesystem. No authentication is required to perform this exploit.
- CVE-2020-15806: Buffer Over-read vulnerability for Festo Controller CECC-S,-LK,-D
  - Specifically crafted requests sent to the CODESYS Control runtime system can allocate arbitrary amounts of memory, causing the system to run out of memory and possibly crash.
- CVE-2021-27478: Incorrect Conversion between Numeric Types Vulnerability in Festo product Ethernet/IP Stack of SBRD-Q/SBOC-Q/SBOI-Q
  - A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
- CVE-2021-27482: Out-of-bounds Read Vulnerability in Festo product Ethernet/IP Stack of SBRD-Q/SBOC-Q/SBOI-Q
  - A specifically crafted packet sent by an attacker may allow the attacker to read arbitrary data.
- CVE-2021-27498: Reachable Assertion Vulnerability in Festo product Ethernet/IP Stack of SBRD-Q/SBOC-Q/SBOI-Q
  - A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
- CVE-2021-27500: Reachable Assertion Vulnerability in Festo product Ethernet/IP Stack of SBRD-Q/SBOC-Q/SBOI-Q
  - A specifically crafted packet sent by an attacker to the affected devices may cause a denial-of-service condition.
- CVE-2021-29242: Improper Input Validation vulnerability for Festo Controller CECC-S,-LK,-D
  - CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages.

- CVE-2021-36763: Files or Directories Accessible to External Parties vulnerability for Festo Controller CECC-S,-LK,-D
  - In CODESYS V3 web server before 3.5.17.10, files or directories are accessible to External Parties.
- CVE-2021-36764: NULL Pointer Dereference vulnerability for Festo Controller CECC-S,-LK,-D
  - In CODESYS Gateway V3 before 3.5.17.10, there is a NULL Pointer Dereference. Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition.
- CVE-2022-1264: Path Traversal in Inductive Automation Ignition
  - The affected product may allow an attacker with access to the Ignition web configuration to run arbitrary code.
- CVE-2022-1704: Improper Restriction of XML External Entity Reference in Inductive Automation Ignition
  - Due to an XML external entity reference, the software parses XML in the backup/restore functionality without XML security flags, which may lead to a XXE attack while restoring the backup.
- CVE-2022-22513: NULL Pointer Dereference vulnerability for Festo Controller CECC-S,-LK,-D
  - The CODESYS protocol communication servers allow authenticated manipulated requests to dereference null pointers or provided untrusted pointers.
- CVE-2022-22514: Untrusted Pointer Dereference vulnerability in Festo Controller CECC-S,-LK,-D
  - An authenticated, remote attacker can gain access to a dereferenced pointer contained in a request. The accesses can subsequently lead to local overwriting of memory in the CmpTraceMgr, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.
- CVE-2022-22515: Exposure of Resource to Wrong Sphere Vulnerability in Festo Controller CECC-S,-LK,-D
  - A remote, authenticated attacker could utilize the control program of the CODESYS Control runtime system to use the vulnerability in order to read and modify the configuration file(s) of the affected products.
- CVE-2022-22517: Small Space of Random Values Vulnerability in Festo Controller CECC-S,-LK,-D
  - An unauthenticated, remote attacker can disrupt existing communication channels between CODESYS products by guessing a valid channel ID and injecting packets. This results in the communication channel to be closed.
- CVE-2022-22519: Buffer Over-read Vulnerability in Festo Controller CECC-S,-LK,-D
  - The CODESYS web server is used by the CODESYS WebVisu to display CODESYS visualization screens in a web browser. Specific crafted HTTP or HTTPS requests may cause an internal buffer over-read, which could crash the web server task of the CODESYS Control runtime system.
- CVE-2022-30308: Incorrect Authorization Vulnerability in Festo Controller CECC-X-M1 Product Family

- In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-web-viewer-request-on” POST request doesn’t check for port syntax. This can result in unauthorized execution of system commands with root privileges due to improper access control command injection.
- CVE-2022-30309: Incorrect Authorization Vulnerability in Festo Controller CECC-X-M1 Product Family
  - In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-web-viewer-request-off” POST request doesn’t check f... result in unauthorized execution of system commands with root privileges due to improper access control command injection.
- CVE-2022-30310: Incorrect Authorization Vulnerability in Festo Controller CECC-X-M1 Product Family
  - In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-acknerr-request” POST request doesn’t check for port... result in unauthorized execution of system commands with root privileges due to improper access control command injection.
- CVE-2022-30311: Incorrect Authorization Vulnerability in Festo Controller CECC-X-M1 Product Family
  - In Festo Controller CECC-X-M1 product family, the http-endpoint “cecc-x-refresh-request” POST request doesn’t check for port... result in unauthorized execution of system commands with root privileges due to improper access control command injection.
- CVE-2022-3079: Improper Privilege Management Vulnerability for Festo products CPX-CEC-C1 and CPX-CMXX
  - Festo control block CPX-CEC-C1 and CPX-CMXX in multiple versions allow unauthenticated, remote access to critical webpage functions which may cause a denial of service.
- CVE-2022-31806: Insecure Default Initialization of Resource vulnerability in Festo products
  - In CODESYS V2 PLCWinNT and Runtime Toolkit 32 in versions prior to V2.4.7.57 password protection is not enabled by default and there is no information or prompt to enable password protection at login in case no password is set at the controller.
- CVE-2022-3270: Insufficient Technical Documentation Vulnerability in Festo Products
  - Incomplete user documentation of remote accessible functions and their required IP ports. The supported features may be covered only partly by the corresponding user documentation. Festo developed the products according to the respective state of the art. As a result, the protocols used no longer fully meet today's security requirements. The products are designed and developed for use in sealed-off (industrial) networks. If the network is not adequately sealed off, unauthorized access to the product can cause damage or malfunctions, particularly Denial of Service (DoS) or loss of integrity.
- CVE-2022-35869: Improper Authentication Bypass in Inductive Automation Ignition
  - This vulnerability allows remote attackers to bypass authentication on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Authentication is not required to exploit this vulnerability. The specific flaw exists within com.inductiveautomation.ignition.gateway.web.pages. The issue results from the lack of proper authentication prior to access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-17211.

- CVE-2022-35870: Deserialization Vulnerability in Inductive Automation Ignition
  - This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within `com.inductiveautomation.metro.impl`. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-17265.
- CVE-2022-35871: Missing Authentication for Critical Function in Inductive Automation Ignition
  - This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). Authentication is not required to exploit this vulnerability. The specific flaw exists within the `authenticateAdSso` method. The issue results from the lack of authentication prior to allowing the execution of python code. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-17206.
- CVE-2022-35872: Deserialization of Untrusted Data RCE in Inductive Automation Ignition
  - This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ZIP files. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-17115.
- CVE-2022-35873: Code Injection via Malformed ZIP in Inductive Automation Ignition
  - This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition 8.1.15 (b2022030114). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of ZIP files. Crafted data in a ZIP file can cause the application to execute arbitrary Python scripts. The user interface fails to provide sufficient indication of the hazard. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-16949.
- CVE-2022-35890: Session ID Predictability in Inductive Automation Ignition
  - An issue was discovered in Inductive Automation Ignition before 7.9.20 and 8.x before 8.1.17. Designer and Vision Client Session IDs are mishandled. An attacker can determine which session IDs were generated in the past and then hijack sessions assigned to these IDs via Randy
- CVE-2022-36126: ScriptInvoke Remote Code Execution in Inductive Automation Ignition
  - An issue was discovered in Inductive Automation Ignition before 7.9.20 and 8.x before 8.1.17. The `ScriptInvoke` function allows remote attackers to execute arbitrary code by supplying a Python script.
- CVE-2022-47378: Improper Validation of Consistency within Input Vulnerability in Festo Products

- After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpFiletransfer component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2022-47379: Out-of-bounds Write Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to memory, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47380: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47381: Stack-based Buffer Overflow for Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47382: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47383: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47384: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47385: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpAppForce component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47386: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47387: Stack-based Buffer Overflow Vulnerability in Festo Products

- After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47388: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47389: Stack-based Buffer Overflow Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47390: Stack-based Buffer Overflow Vulnerability in in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.
- CVE-2022-47391: Improper Validation of Consistency within Input Vulnerability in Festo Products
  - CODESYS products such as the CODESYS Control runtime systems contain communication servers for the CODESYS protocol to enable the CmpDevice component to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2022-47392: Improper Validation of Consistency within Input Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpApp/CmpAppBP/CmpAppForce components to read internally from an invalid address, potentially leading to a denial-of-service condition.
- CVE-2022-47393: Untrusted Pointer Dereference Vulnerability in Festo Products
  - After successful authentication, specific crafted communication requests can cause the CmpFiletransfer component to dereference addresses provided by the request for internal read access, which can lead to a denial-of-service situation.
- CVE-2023-3634: Hidden Functionality Vulnerability for Festo products MSE6-C2M/D2M/E2M
  - In products of the MSE6 product-family by Festo a remote authenticated, low privileged attacker could use functions of undocumented test mode which could lead to a complete loss of confidentiality, integrity and availability.
- CVE-2023-38121: Dangerous Method Exposure in Inductive Automation Ignition
  - Inductive Automation Ignition OPC UA Quick Client Cross-Site Scripting Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the id parameter provided to the Inductive Automation Ignition web

interface. The issue results from the lack of proper validation of user-supplied data, which can lead to the injection of an arbitrary script. An attacker can leverage this vulnerability to execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-20355.

- CVE-2023-38122: Improper Authentication in Inductive Automation Ignition
  - Inductive Automation Ignition OPC UA Quick Client Permissive Cross-domain Policy Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the configuration of the web server. The issue results from the lack of appropriate Content Security Policy headers. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of SYSTEM. Was ZDI-CAN-20539.
- CVE-2023-38123: Cross-Site Scripting in Inductive Automation Ignition
  - Inductive Automation Ignition OPC UA Quick Client Missing Authentication for Critical Function Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the server configuration. The issue results from the lack of authentication prior to allowing access to password change functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-20540.
- CVE-2023-38124: Dangerous Method Exposure in Inductive Automation Ignition
  - Inductive Automation Ignition OPC UA Quick Client Task Scheduling Exposed Dangerous Function Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the Ignition Gateway server. The issue results from the exposure of a dangerous function. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-20541.
- CVE-2023-39472: XXE Vulnerability in Inductive Automation Ignition
  - Inductive Automation Ignition SimpleXMLReader XML External Entity Processing Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the SimpleXMLReader class. Due to the improper restriction of XML External Entity (XXE) references, a crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of the SYSTEM. Was ZDI-CAN-17571.
- CVE-2023-39473: Unsafe Java Deserialization in Inductive Automation Ignition
  - Inductive Automation Ignition AbstractGatewayFunction Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this

vulnerability. The specific flaw exists within the AbstractGatewayFunction class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. . Was ZDI-CAN-17587.

- CVE-2023-39474: downloadLaunchClientJar RCE in Inductive Automation Ignition
  - Inductive Automation Ignition downloadLaunchClientJar Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must connect to a malicious server. The specific flaw exists within the downloadLaunchClientJar function. The issue results from the lack of validating a remote JAR file prior to loading it. An attacker can leverage this vulnerability to execute code in the context of the current user. . Was ZDI-CAN-19915.
- CVE-2023-39475: Critical Deserialization in Inductive Automation Ignition
  - Inductive Automation Ignition ParameterVersionJavaSerializationCodec Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is not required to exploit this vulnerability. The specific flaw exists within the ParameterVersionJavaSerializationCodec class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-20290.
- CVE-2023-39476: Privilege Escalation in Inductive Automation Ignition
  - Inductive Automation Ignition JavaSerializationCodec Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is not required to exploit this vulnerability. The specific flaw exists within the JavaSerializationCodec class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-20291.
- CVE-2023-39477: OPC UA Server DoS in Inductive Automation Ignition
  - Inductive Automation Ignition ConditionRefresh Resource Exhaustion Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of Inductive Automation Ignition. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of OPC UA ConditionRefresh requests. By sending a large number of requests, an attacker can consume all available resources on the server. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-20499.
- CVE-2023-50218: Insecure Deserialization in Inductive Automation Ignition
  - Inductive Automation Ignition ModuleInvoke Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on

affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the ModuleInvoke class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-21624.

- CVE-2023-50219: RunQuery Deserialization RCE in Inductive Automation Ignition
  - Inductive Automation Ignition RunQuery Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the RunQuery class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-21625.
- CVE-2023-50220: Base64Element Deserialization RCE in Inductive Automation Ignition
  - Inductive Automation Ignition Base64Element Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the Base64Element class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-21801.
- CVE-2023-50221: ExtendedDocumentCodec Deserialization in Inductive Automation Ignition
  - Inductive Automation Ignition ResponseParser SerializedResponse Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must connect to a malicious server. The specific flaw exists within the ResponseParser method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-21926.
- CVE-2023-50222: Directory Traversal in Inductive Automation Ignition
  - Inductive Automation Ignition ResponseParser Notification Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must connect to a malicious server. The specific flaw exists within the ResponseParser method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-22067.
- CVE-2023-50223: getJavaExecutable Path Traversal in Inductive Automation Ignition

- Inductive Automation Ignition ExtendedDocumentCodec Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. Authentication is required to exploit this vulnerability. The specific flaw exists within the ExtendedDocumentCodec class. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-22127.
- CVE-2023-50232: Code Injection via Argument Injection in Inductive Automation Ignition
  - Inductive Automation Ignition getParams Argument Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must connect to a malicious server. The specific flaw exists within the getParams method. The issue results from the lack of proper validation of a user-supplied string before using it to prepare an argument for a system call. An attacker can leverage this vulnerability to execute code in the context of the current user. Was ZDI-CAN-22028.
- CVE-2023-50233: Insecure Deserialization in Inductive Automation Ignition
  - This vulnerability allows remote attackers to execute arbitrary code on affected installations of Inductive Automation Ignition. User interaction is required to exploit this vulnerability in that the target must connect to a malicious server. The specific flaw exists within the getJavaExecutable method. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.
- CVE-2024-27088: Perspective Module Dependency Vulnerability in Inductive Automation Ignition
  - es5-ext contains ECMAScript 5 extensions. Passing functions with very long names or complex default argument names into `function#copy` or `function#toStringTokens` may cause the script to stall.
- CVE-2025-13911: Windows Service Excessive Permissions in Inductive Automation Ignition
  - Windows service excessive permissions allowing SYSTEM-level script execution via malicious project import in all Ignition 8.1.x and 8.3.x on Windows with default installation. An authenticated privileged user can import a project file containing Python scripts that execute with the same permissions as the Ignition Gateway process.

## 20260116

### Snort rules

This release includes additions and modifications to the Snort ruleset covering the following Talos advisory:

- **Talos Rules 2026-01-15** (<https://www.snort.org/advisories/talos-rules-2026-01-15>)

- **Talos Rules 2026-01-13** (<https://www.snort.org/advisories/talos-rules-2026-01-13>)

The new and updated Snort rules span the following categories:

- 1 browser-ie rule with SID 301375
- 6 file-multimedia rules with SIDs 65696, 65698, 65697, 65695, 65691, 65690
- 1 file-other rule with SID 301308
- 2 malware-cnc rules with SIDs 65685, 65684
- 1 malware-tools rule with SID 65679
- 8 os-windows rules with SIDs 301374, 301371, 301368, 301369, 301370, 301344, 301373, 301372
- 1 policy-other rule with SID 65689
- 19 server-webapp rules with SIDs 65660, 65659, 65678, 65661, 65662, 65681, 65677, 65686, 21517, 65693, 65657, 45570, 65694, 65658, 65682, 65683, 65680, 65692, 37415

## Vulnerabilities

This release adds support and modifications for the detection of the following vulnerabilities:

- CVE-2025-40805: Authorization Bypass Vulnerability in Siemens Industrial Edge Devices, SCALANCE LPE9413, SCALANCE LPE9433 and other products
  - Affected devices do not properly enforce user authentication on specific API endpoints. This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user. Successful exploitation requires that the attacker has learned the identity of a legitimate user.
- CVE-2025-40944: Denial-of-Service Vulnerability in Siemens SIMATIC ET 200AL, SIMATIC ET 200MP, SIMATIC ET 200SP and other products
  - Affected devices do not properly handle S7 protocol session disconnect requests. When receiving a valid S7 protocol Disconnect Request (COTP DR TPDU) on TCP port 102, the devices enter an improper session state. This could allow an attacker to cause the device to become unresponsive, leading to a denial-of-service condition that requires a power cycle to restore normal operation.
- CVE-2025-41717: Code Injection Vulnerability in Phoenix Contact TC ROUTER and CLOUD CLIENT Industrial mobile network routers
  - A code injection vulnerability at the upload-config endpoint in the firmware of TC ROUTER and CLOUD CLIENT Industrial Mobile network routers has been discovered that can be exploited by an high privileged attacker.

## 20260109

## Snort rules

This release includes additions and modifications to the Snort ruleset covering the following Talos advisory:

- **Talos Rules 2026-01-08** (<https://www.snort.org/advisories/talos-rules-2026-01-08>)
- **Talos Rules 2026-01-06** (<https://www.snort.org/advisories/talos-rules-2026-01-06>)
- **Talos Rules 2025-12-30** (<https://www.snort.org/advisories/talos-rules-2025-12-30>)
- **Talos Rules 2025-12-23** (<https://www.snort.org/advisories/talos-rules-2025-12-23>)

The new and updated Snort rules span the following categories:

- 1 browser-other rule with SID 301367
- 12 file-multimedia rules with SIDs 65639, 65623, 65622, 65621, 65650, 65651, 65642, 65620, 65641, 65652, 65638, 65649
- 1 file-other rule with SID 301365
- 15 malware-cnc rules with SIDs 65634, 65637, 65631, 65654, 65655, 65656, 65632, 65629, 65630, 65633, 65640, 301185, 65617, 65645, 65644
- 1 malware-other rule with SID 301366
- 2 policy-other rules with SIDs 65653, 65646
- 1 protocol-other rule with SID 65624
- 6 server-webapp rules with SIDs 62935, 65619, 65628, 65625, 65618, 65643