National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15

Report Number: CCEVS-VR-VID11603-2025
Dated: October 3, 2025
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Clare Parran
Sheldon Durrant
Lori Sarem
Randy Heimann
The MITRE Corporation

Michael Smeltzer
Johns Hopkins APL

Common Criteria Testing Laboratory

Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 1
3 Architectural Information 3
3.1 TOE Description 3
3.2 TOE Evaluated Platforms 3
3.3 TOE Architecture 3
3.4 Physical Boundaries 4
4 Security Policy 4
4.1 Security audit 5
4.2 Cryptographic support 5
4.3 Identification and authentication 6
4.4 Security management 6
4.5 Protection of the TSF 7
4.6 TOE access 7
4.7 Trusted path/channels 7
5 Assumptions & Clarification of Scope 8
6 Documentation 9
7 IT Product Testing 9
7.1 Developer Testing 9
7.2 Evaluation Team Independent Testing 9
8 TOE Evaluated Configuration 9
8.1 Evaluated Configuration 9
8.2 Excluded Functionality 10
9 Results of the Evaluation 10
9.1 Evaluation of the Security Target (ASE) 10
9.2 Evaluation of the Development (ADV) 11
9.3 Evaluation of the Guidance Documents (AGD) 11
9.4 Evaluation of the Life Cycle Support Activities (ALC) 11
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 11
9.6 Vulnerability Assessment Activity (VAN) 12
9.7 Summary of Evaluation Results 12
10 Validator Comments/Recommendations 13
11 Annexes 13
12 Security Target 13
13 Glossary 13
14 Bibliography 14

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in October 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices and MACsec Ethernet Encryption, version 2.0, 25 April 2024 (CFG_NDcPP-MACsec_V2.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2 March 2023 (MACsec10) and the *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10).

The Target of Evaluation (TOE) is the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). The validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Security Target, version 1.0, October 1, 2025 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product

evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Network Devices and MACsec Ethernet Encryption, version 2.0, 25 April 2024* (CFG_NDcPP-MACsec_V2.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e) with the *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2 March 2023 (MACsec10) and the *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)
ST	*Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Security Target*, version 1.0, October 1, 2025
Evaluation Technical Report	*Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15*, version 0.3, October 1, 2025
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD

Item	Identifier
CCEVS Validators	The MITRE Corporation, Johns Hopkins APL

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST.

The TOE is the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 all running Internetworking Operating System (IOS)-XE 17.15. The TOE is a purpose-built, switching and routing platform with Open System Interconnection (OSI) Layer2 and Layer3 traffic filtering capabilities. The TOE also supports Media Access Control Security (MACsec) encryption for switch-to-switch (inter-network device) security.

3.1 TOE Description

The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 are switching and routing platforms that provide connectivity and security services, including MACsec encryption, on a single, secure device. These switches offer broadband speeds and simplified management to small businesses, enterprise small branch, and teleworkers.

The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches are single-device security and switching solutions for protecting the network.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches Target of Evaluation (TOE) is comprised of both software and hardware. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.15. The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. The Cisco Catalyst Industrial Ethernet IE9300 Rugged Series Switches primary features include the following:

- Central processor that supports all system operations.
- Full Gigabit Ethernet switch:
  - Total of 28 Gigabit Ethernet ports provide multiple resilient design options
  - Provides secure access for new high-speed applications in the industrial space
- Memory:
  - 4-GB DRAM
  - 8-GB onboard flash memory

- Available Interfaces:
  - USB 2.0 (all models)
  - RS-232 (via RJ-45) and 1 Micro USB Console Interfaces (all models)
    - Note: an RJ-45-to-DB-9 adapter cable is supplied to be used to connect the console port of the switch to a console PC.
  - **IE-9310-26S2C, IE-9320-26S2C**
    - 22 100/1000M SFP fiber ports
    - 2 Combo (100/1000M SFP, 10/100/1000M RJ-45) ports
    - 4 1G SFP fiber ports
  - **IE-9320-22S2C4X**
    - 22 100/1000M SFP fiber ports
    - 2 Combo (100/1000M SFP, 10/100/1000M RJ-45) ports
    - 4 1/10G SFP+ fiber ports
  - **IE-9320-24P4S**
    - 24 10/100/1000M RJ-45 PoE+
    - 4 1G SFP fiber ports
  - **IE-9320-24T4X**
    - 24 10/100/1000M RJ-45
    - 4 1/10G SFP+ fiber ports
  - **IE-9320-24P4X**
    - 24 10/100/1000M RJ-45 PoE+
    - 4 1/10G SFP+ fiber ports
  - **IE-9320-16P8U4X**
    - 16 10/100/1000M PoE+
    - 8 Combo (100/1000/2500M 4PPoE)
    - 4 1/10G SFP+ fiber ports

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 4 below.

3.4 Physical Boundaries

The TOE is a hardware and software solution that makes up the switch models.

The network on which they reside is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.15. In addition, the software image is also downloadable from the Cisco web site. A login id and password are required to download the software image.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support

3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The Cisco Catalyst IE9300 Rugged Series Switches provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server.

The TOE also internally stores audit records in a circular log file where the oldest audit records are overwritten when the audit trail becomes full. The audit logs can be viewed on the TOE using the appropriate IOS-XE 17.15 commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the Authorized Administrator to clear audit data stored locally on the TOE.

4.2 Cryptographic support

The TOE provides the cryptography to support all security functions. All algorithms claimed have Cryptographic Algorithm Validation Program (CAVP) certificates.

The TOE leverages the IOS Common Cryptographic Module (IC2M), firmware version Rel5a (CAVP cert. #A1462).

The TOE supports MACsec using the proprietary UAPD MSC MACsec embedded in ASICs v1.1 (CAVP Cert. #4848).

The TOE provides cryptographic support for IPsec, which is used to secure the session between the TOE and the audit server. The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

Refer to the ST for detailed information on the mapping of certificates and cryptographic methods to TOE functionality.

4.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (TOE peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure Command Line Interface (CLI) Administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides Administrator authentication against a local user database. Password-based authentication can be performed on the local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of failed authentication attempts has exceeded the configured allowable attempts, the user is locked out until an Authorized Administrator can reenable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.

4.4 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local serial console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely
- Configuration of warning and consent access banners
- Configuration of session inactivity thresholds
- Updates of the TOE software
- Configuration of authentication failures
- Configuration of the audit functions of the TOE
- Configuration of the TOE provided services
- Configuration of the cryptographic functionality of the TOE
- Generate, install, and manage Pre-Shared Key (PSK)
- Manage the Key Server, Connectivity Association Key (CAK) and MKA participants
- Configure lockout time interval for excessive authentication failures

The TOE supports two separate Administrator roles: non-privileged Administrator and privileged Administrator. Only the privileged Administrator can perform the above security relevant management functions. The privileged Administrator is the Authorized Administrator of the TOE who can enable, disable, determine, and modify the behaviour of the security functions of the TOE as described in this document.

4.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

The TOE can verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

The TOE detects replay of information received via secure channels (MACsec). The detection is applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time information is used as the timestamp that is applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to update the TOE's clock manually to maintain a reliable timestamp.

Finally, the TOE performs testing to verify correct operation of the TOE itself and that of the cryptographic module.

4.6 TOE access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4.7 Trusted path/channels

The TOE allows a trusted path to be established to itself from remote Administrators over SSHv2 and initiates outbound IPsec trusted channels to transmit audit messages to remote syslog servers. In addition, IPsec is used as a trusted channel between the TOE and the remote authentication servers.

The TOE supports MACsec secured trusted channels between itself and MACsec peers.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e)
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2 March 2023 (MACsec10)
- *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/MACsec10/SSH10 should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/MACsec10/SSH10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices with the MACsec PP-Module and SSH Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Device, MACsec Ethernet Encryption models was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP30e/MACsec10/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 CC Configuration Guide*, Version 0.3, September 26, 2025

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Detailed Test Report for Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15*, Version 0.2, September 29, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e/MACsec10/SSH10 including the tests associated with optional requirements. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

This section briefly identifies the evaluated configuration(s) and any excluded and out of scope functionality.

8.1 Evaluated Configuration

The evaluation includes the following hardware models:

- IE-9310-26S2C
- IE-9320-26S2C
- IE-9320-22S2C4X

- IE-9320-24T4X
- IE-9320-24P4X
- IE-9320-24P4S
- IE-9320-16P8U4X

8.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
Transport Layer Security (TLS)	TLS is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
Hypertext Transfer Protocol (HTTP)	Remote Management is performed using SSH
Hypertext Transfer Protocol Secure (HTTPS)	Remote Management is performed using SSH
TOE Peer (Conditional)	If the remote syslog server is directly connected to the TOE for the TOE's use, then the TOE Peer is not required.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP30e/MACsec10/SSH10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation

was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP30e/MACsec10/SSH10 related to the examination of the information contained in the TSS.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e/MACsec10/SSH10 and recorded the results in a Test Report, summarized in the AAR.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation

was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team performed a public search against the following sources to ensure there are no publicly known and exploitable vulnerabilities in the TOE:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search, ref NVD)
- MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php, ref CVE),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/, ref VND),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities, ref Rapid7)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories, ref ZDI)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search, ref TEN)
- Offensive Security Exploit Database (https://www.exploit-db.com/, ref EDB

The search was performed most recently on September 15, 2025 and conducted with the following search terms:: “IC2M”, “IOS Common Cryptographic Module”, “Unified Access Data Plane”, “UADP”, “Cisco Catalyst”, “IOS-XE 17.15”, “Cisco IOS XE 17.15”, “MACsec”, “MACsec Controller”, “MSC”, “IE-9310-26S2C”, “IE-9320-26S2C”, “IE-9320-22S2C4X”, “IE-9320-24T4X”, “IE-9320-24P4X”, “IE-9320-24P4S”, “IE-9320-16P8U4X”, “ARM Cortex-A53”, “ARMv8 Cortex A53”.

The *validation team* reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 CC Configuration Guide*, Version 0.3, September 15, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the CFG_NDcPP-MACsec_V2.0 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Security Target, Version 1.0, October 1, 2025*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent,

technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e).

[5] *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 2 March 2023 (MACsec10).

[6] *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10).

[7] *Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Security Target*, Version 1.0, October 1, 2025 (ST).

[8] *Assurance Activity Report for Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15*, Version 0.3, October 1, 2025 (AAR).

[9] *Detailed Test Report for Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15*, Version 0.2, September 29, 2025 (DTR).

[10] *Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15*, Version 1.0, October 1, 2025 (ETR).