National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cisco Systems, Inc. Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12

Report Number: CCEVS-VR-VID11463-2024
Dated: August 20, 2024
Version: 0.3

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

Jerome Myers
Meredith M Martinez
Seada Mohammed
The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Allison Keenan
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 solution provided by Cisco Systems, Inc.. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 July 2024. 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 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v2.0) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10).

The Target of Evaluation (TOE) is the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report 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 evaluation technical report 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). Therefore 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 Security Target, version 0.9, July 29, 2024 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 9300/9300L/9400/9500/9600 Series Switches 17.12 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 29 March 2023 (CFG_NDcPP-MACsec_v2.0) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)
ST	Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 Security Target, version 0.9, July 29, 2024
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12, version 0.3, July 29, 2024
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
CCEVS Validators	Jerome Myers, Meredith M Martinez, Seada Mohammed

3 Architectural Information

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

The Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 Target of Evaluation (TOE) is an enterprise access and core/distribution switch for enterprise and campus deployments. Switches are used to connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other and are key building blocks for any network.

3.1 TOE Description

The Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 TOE is a purpose-built, switching and routing platform enabling connected devices to communicate over a network at layer 2 or 3. The TOE provides Administrative control and management of the network. For communicating with other network devices, the TOE provides AES-128 and AES-256 MACsec encryption. The TOE also provides Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access.

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

Deployment of the TOE in its evaluated configuration consists of at least one TOE switch model following the CC installation and configuration guidance document (AGD). The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internet working device and forwarded to their configured destination.

The TOE can be administered interactively using a CLI over a local console connection or remotely over SSH.

The operational environment of the TOE will include at least one MACsec peer. The environment will also include an audit (syslog) server and a Management Workstation. The syslog server is used to store audit records, where the TOE uses IPsec to secure the transmission of the records.

3.4 Physical Boundaries

The TOE is a hardware and software solution that makes up the switch models as follows: Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running Cisco IOS-XE 17.12. The network on which they reside is considered part of the environment. 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

3.5 Security audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The TOE stores audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with IPsec.

3.6 Cryptographic support

The TOE provides cryptographic functions to implement SSH, IPsec, and MACsec protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation.

The TOE supports MACsec using the proprietary Unified Access Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC). The MACsec Controller (MSC) v1.0 is embedded within the ASICs that are utilized within Cisco hardware platforms.

SSH and IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) version Rel5a cryptographic modules. Refer to Table 21 of the ST for identification of the relevant CAVP certificates.

3.7 Identification and authentication

The TOE implements three types of authentication to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication for remote syslog servers, password-based authentication for Security Administrators, and pre-shared keys for MACsec endpoints.

Security Administrators have the ability to compose strong passwords which are stored using a SHA-2 hash. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator defined time period has elapsed or until the Administrator manually unblocks the account.

3.8 Security management

The TOE provides secure remote administrative interface and local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination as well as an ability to update TOE software.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

3.9 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

3.10 TOE access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

3.11 Trusted path/channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

4 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 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)

That information has not been reproduced here and the NDcPP22e/MACsec10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/MACsec10 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.

Clarification of scope

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 and the MACsec Module 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 MACsec Ethernet Encryption models was not included in the scope of the evaluation and therefore should not to 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 NDcPP22e/MACsec10 and applicable Technical

Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, as identified in Table 4 of the Security Target, the following functionality is explicitly excluded from the scope of the evaluation:

- Non-FIPS 140-2 mode of operation
- HTTP/HTTPS and
- SNMP

These services can be disabled by using the configuration settings as described in the Administrative Guidance Documents (AGD).

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e or the PP-Module for MACsec Ethernet Encryption v1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

5 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 CC Configuration Guide, Version 0.7, July 16, 2024

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to 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.

6 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 9300/9300L/9400/9500/9600 Series Switches 17.12, Version 0.3, July 29, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

6.1 Developer Testing

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

6.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACsec10 including the tests associated with optional requirements. The AAR, in section 3.5.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

7 Evaluated Configuration

The TOE is a hardware and software solution that makes up the switch models as follows: Catalyst 9300/9300L/9400/9500/9600 Series Switches running Cisco IOS-XE 17.12.

Series	Models
Catalyst 9300 Hardware Models:	***Chassis:*** C9300-24T, C9300-48T, C9300-24P, C9300-48P, C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN, C9300-24S, C9300-48S, C9300D-24UB, C9300D-48UB, C9300D-24UXB, C9300-24H, C9300-48H ***With the following network modules***: C9300-NM-4G, C9300-NM-8X, C9300-NM-2Q, C9300-NM-4M, C9300-NM-2Y
Catalyst 9300L Hardware Models:	***Chassis:*** C9300L-24T-4G, C9300L-48T-4G, C9300L-24P-4G, C9300L-48P-4G, C9300L-24T-4X, C9300L-48T-4X, C9300L-24P-4X, C9300L-48P-4X, C9300L-48PF-4G, C9300L-48PF-4X, C9300L-24UXG-4X, C9300L-24UXG-2Q, C9300L-48UXG-4X, C9300L-48UXG-2Q
Catalyst 9400 Hardware Models:	***Chassis:*** C9404R, C9407R, C9410R ***With the following Supervisor models:*** C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y ***With the following Line Card models*:** C9400-LC-24S, C9400-LC-48S, C9400-LC-24XS, C9400-LC-48P, C9400-LC-48T, C9400-LC-48U, C9400-LC-48UX, C9400-LC-48H
Catalyst 9500 Hardware Models:	***Chassis:*** C9500-16X, C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C ***With the following network modules:*** C9500-NM-8X, C9500-NM-2Q
Catalyst 9600 Hardware Models:	***Chassis:*** C9606R ***With the following Supervisor models:*** C9600-SUP-1 ***With the following Line Card models:*** C9600-LC-24C, C9600-LC-48YL, C9600-LC-48TX, C9600-LC-24S

8 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 Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsec10.

8.1 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 9300/9300L/9400/9500/9600 Series Switches 17.12 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

8.2 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 NDcPP22e/MACsec10 related to the examination of the information contained in the TSS.

The validator 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.

8.3 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 validator 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.

8.4 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 validator 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.

8.5 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 NDcPP22e/MACsec10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

8.6 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 evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 7/29/2024 with the following search terms: “SSH”, “IPsec”, “IKE”, “MACsec”, “MACsec Controller”, “MSC”, “IC2M”, “IC2M Rel5a”, “IOS Common Cryptographic Module”, “Unified Access Data Plane”, “UADP”, “Cisco Catalyst”, “C9300”, “C9300L”, “C9400”, “C9404R”, “C9407R”, “C9410R”, “C9400-SUP”, “C9400-LC”, “C9500”, “C9600”, “C9606R”, “C9600-SUP”, “C9600-LC”, “Catalyst 9300”, “Catalyst 9300L”, “Catalyst 9400”, “Catalyst 9404R”, “Catalyst 9407R”, “Catalyst 9410R”, “Catalyst 9500”, “Catalyst 9600”, “Catalyst 9606R”, “IOS-XE 17.12”, “Cisco IOS XE 17.12”, “Intel Xeon D-1523N”, “Intel Xeon D-1530”, “Intel Xeon D-1526”, “Intel Xeon D-1548”, “Intel Atom C3558”, “Intel Broadwell processor”, “Intel Goldmont processor”.

The validator 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.

8.7 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.

9 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 9300/9300L/9400/9500/9600 Series Switches 17.12 CC Configuration Guide, Version 0.7, July 16, 2024.

No versions of the TOE and software, either earlier or later are covered by the scope of this evaluation. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 5 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as: Cisco *Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 Security Target, Version 0.9, July 29, 2024*.

12 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.

13 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 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10).

[6] Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12 Security Target, Version 0.9, July 29, 2024 (ST).

[7] Assurance Activity Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12, Version 0.3, July 29, 2024 (AAR).

[8] Detailed Test Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12, Version 0.3, July 29, 2024 (DTR).

[9] Evaluation Technical Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 17.12, Version 0.3, July 29, 2024 (ETR).