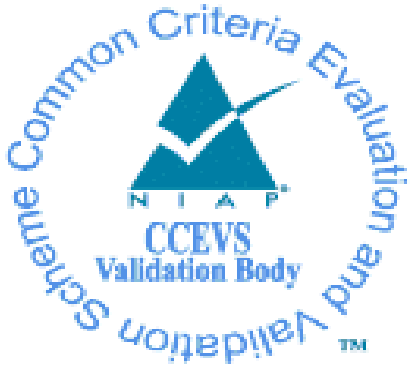
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12

Report Number: CCEVS-VR-VID11521-2025
Dated: March 13, 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

Lisa Mitchell
Jenn Dotson
Sheldon Durrant
Randy Heimann
Lori Sarem
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Linh Le
Douglas Kalmus
Catherine Sykes
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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 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 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 March 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 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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12.

The Target of Evaluation (TOE) identified in this VR 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 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 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). 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 *Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 Security Target*, version 1.0, March 10, 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 Product Compliant 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 results 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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 Security Target*, version 1.0, March 10, 2025
Evaluation Technical Report	*Evaluation Technical Report for Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12*, version 0.2, March 10, 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.

Item	Identifier
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	The MITRE Corporation

3 Architectural Information

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

The Cisco Embedded Services 9300 and 3300 Series Switches are purpose-built, switching platforms that also supports MACsec and IPsec encryption.

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

3.1 TOE Description

The TOE is comprised of both software and hardware. The hardware is comprised of industry-standard small form factor cards which provide a compact, modular, and customizable solution. The hardware models included in the evaluation are: ESS-3300-NCP, ESS-3300-CON, ESS-3300-24T-NCP, ESS-3300-24T-CON and ESS-9300-10X-E. The software is comprised of the Cisco IOS-XE 17.12.

The ESS9300 and ESS3300 models provide secure Layer 2 switching using Enterprise-grade Cisco IOS-XE switching security features to ensure highly secure data communication. The products feature a robust industrial design and support Power over Ethernet.

3.2 TOE Evaluated Platforms

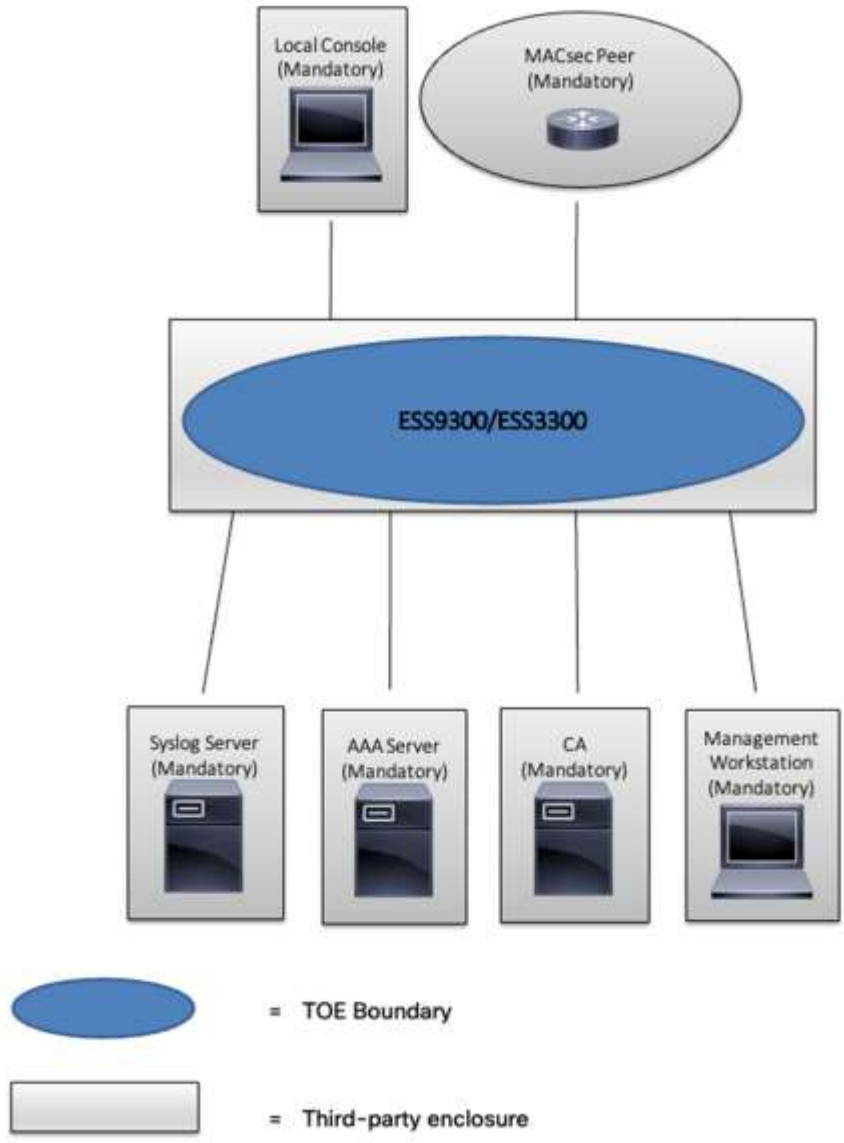
Details regarding the evaluated configuration is provided in Section 8 below.

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 consists of one or more physical devices and includes the Cisco IOS-XE software. 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 internetworking 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, a RADIUS 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. The RADIUS server is used for remote authentication, where the TOE uses IPsec to secure the transmission of data related to remote authentication. The Management Workstation is used for remote management of the TOE by an Administrator, where the TOE uses SSH to secure transmission of management sessions.



3.4 Physical Boundaries

The TOE is a hardware and software solution.

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 17.12. In addition, the software image is also downloadable from the Cisco website. 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

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.

4.2 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 provides cryptographic support for remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers. SSH and

IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) version Rel5a cryptographic modules.

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.

The ESS3300 supports MACsec using the Broadcom BCM54194 a fully integrated octal Gigabit transceiver with standards-compliant IEEE 802.1AE 256bit MACsec functionality (Cert # AES 4544). The tested environment is AES ECB 128bit & 256bit Encryption/Decryption Engine.

The ESS9300 supports MACsec using the proprietary Unified Access Data Plane (UADP) MSC version 1.1 (Cert. # AES 4848). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms. The tested environment is Synopsys VCS v2011.12mx-SP1-3.

4.3 Identification and authentication

The TOE implements three types of authentications to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication per RFC 5280 for IPSec connections to remote syslog or RADIUS AAA servers, password-based and public key based (SSH) 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 provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts exceeding the configured allowable attempts within a configured time interval, the user or administrators account is locked out until the configured amount of time has passed.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. The TOE supports the use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

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 console connection. The TOE provides the ability to securely:

- Administer the TOE locally and remotely;

- Configure the access banner;
- Configure the session inactivity time before session termination or locking;
- Update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Configure the authentication failure parameters for FIA_AFL.1;
- Configure the number of failed administrator authentication attempts that will cause an account to be locked out and how long they will be locked out for;
- Configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full);
- Manage the cryptographic keys;
- Configure the cryptographic functionality;
- Configure thresholds for SSH rekeying;
- Configure the lifetime for IPsec SAs;
- Set the time which is used for time-stamps;
- Configure the reference identifier for the peer;
- Manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Import X509.v3 certificates to the TOE's trust store;
- Manage the trusted public keys database;
- Manage a PSK-based CAK and install it in the device;
- Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XkayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];
- Specify a lifetime of a CAK;
- Enable, disable, or delete a PSK-based CAK using CLI management commands.

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. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authorized administrators.

4.5 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE prevents reading of cryptographic keys and passwords. 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.

Whenever a self-test failure occurs within the TOE, the TOE ceases operation (crashes). In the event of a crash appropriate information is displayed on the console screen and saved in the crashinfo file.

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.

4.6 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. Sessions can also be terminated by an Authorized Administrator.

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

4.7 Trusted path/channels

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

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE also supports MACsec secured trusted channels between itself and MACsec peers.

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.

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 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 for additional information.

Clarification of scope

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.

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 and supplemental information, additional customer documentation for the specific 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 NDcPP22e/MACsec10 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 Embedded Services 3300 and 9300 Series Switches (ESS3300 & ESS9300) running IOS-XE 17.12 Common Criteria Configuration Guide*, version 1.0, March 10, 2025
- *Cisco Embedded Service 9300 Series Switches Configuration Guide*, January 4, 2023
- *Cisco Embedded Services 3300 Series Configuration*, October 23, 2023

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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12, version 0.2, March 10, 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 NDcPP22e/MACsec10 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

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 evaluated configuration includes the following models, configured as specified in the Guidance Documentation listed in Section 6:

- ESS-3300-NCP
- ESS-3300-CON
- ESS-3300-24T-NCP
- ESS-3300-24T-CON
- ESS-9300-10X-E

8.2 Excluded Functionality

The following functionality is excluded from the evaluation:

Excluded Functionality	Exclusion Rationale
USB console access	USB console access was not tested. The RS-232 RJ45 console port was used during testing.
USB Host interface for USB Flash Memory Device	USB Host interface for USB Flash Memory Device was not tested and is not required.

Transport Layer Security (TLS)	TLS is not associated with Security Functional Requirements claimed in [NDcPP]. Use tunnelling through IPsec.
HTTP/HTTPS	Remote Management is performed using SSH
SNMP	Remote Management is performed using SSH
Telnet	Telnet for management purposes is enabled by default and must be disabled in the evaluated configuration. Remote Management is performed using SSH

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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsec10.

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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 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 NDcPP22e/MACsec10 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 NDcPP22e/MACsec10 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),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search),
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was performed on March 8, 2025. The search was conducted with the following search terms: “Cisco IOS XE”, “Cisco Embedded Services”, “ESS-3300-NCP”, “ESS-3300-CON”, “ESS-3300-24T-NCP”, “ESS-3300-24T-CON”, “ESS-9300-10X-E”, “Xilinx ZU3EG”, “Broadcom BCM54194”, “CrayCore”, “MSC MACsec”, “IOS Common Cryptographic Module”, and “IC2M”.

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 Embedded Services 3300 and 9300 Series Switches (ESS3300 & ESS9300) running IOS-XE 17.12 Common Criteria Configuration Guide*, version 1.0, March 10, and accompanying supplemental configuration guides. 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 NDcPP22e/MACsec10 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 Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 Security Target*, version 1.0, March 10, 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 2.2e, 23 March 2020 (NDcPP22e).

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

[6] *Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12 Security Target*, version 1.0, March 10, 2025 (ST).

[7] *Assurance Activity Report for Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12*, version 0.2, March 10, 2025 (AAR).

[8] *Detailed Test Report for Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12*, version 0.2, March 10, 2025 (DTR).

[9] *Evaluation Technical Report for Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.12*, version 0.2, March 10, 2025 (ETR).

[10] *Cisco Embedded Services 3300 and 9300 Series Switches (ESS3300 & ESS9300) running IOS-XE 17.12 Common Criteria Configuration Guide*, version 1.0, March 10, 2025

[11] *Cisco Embedded Service 9300 Series Switches Configuration Guide*, January 4, 2023

[12] *Cisco Embedded Services 3300 Series Configuration*, October 23, 2023