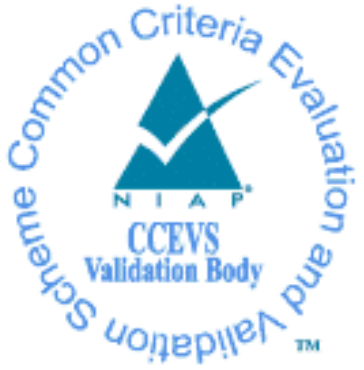
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
Cisco Systems, Inc. Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9

Report Number: CCEVS-VR-VID11365-2023
Dated: July 18, 2023
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

Viet Hung Le
Meredith Martinez
Elizabeth Scruggs
Chris Thorpe

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Khai Van
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 running IOS-XE 17.9 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 2023. 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 collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e) with the Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016 (MACsecEP12).

The Target of Evaluation (TOE) is the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9.

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 Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 Common Criteria Security Target, version 0.5, July 17, 2023 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 running IOS-XE 17.9 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016
ST	Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 Common Criteria Security Target, version 0.5, July 17, 2023
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9, version 0.2, July 17, 2023
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	Viet Hung Le, Meredith Martinez, Elizabeth Scruggs, Chris Thorpe

3 Architectural Information

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

The TOE is the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches all running Internetworking Operating System (IOS)-XE 17.9. 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.

The TOE is comprised of both software and hardware. The software is comprised of the Universal Cisco IOS-XE. Hardware models only vary in component characteristics. These characteristics affect non-security relevant functions, such as throughput and amount of storage. Since there is no security relevant impact due to differing components, equivalence between all switch models is claimed.

Primary features of the Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches include the following:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Central Processing Unit (CPU) complex with 8-GigaBytes (GB) memory, 16-GB of flash, and an external Universal Serial Bus (USB) 3.0 Solid State Drive (SSD) pluggable storage slot (delivering 120-GB of storage with an optional SSD drive)
- Serial Advanced Technology Attachment (SATA) SSD local storage
- Flash memory Electrically Erasable Programmable Read-Only Memory (EEPROM), used to store the Cisco IOS-XE image (binary program)
- Non-volatile Read Only Memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile Random-Access Memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up
- Physical network interfaces (minimally two) (e.g., Registered Jack (RJ-45) serial and standard 10/100/1000 Ethernet ports). The number of network interface ports varies by model
- Dedicated management port on the switch, RJ-45 console port, and a USB mini-Type B console connection
- Resiliency with Field Replaceable Units (FRU) and redundant power supply, fans, and modular uplinks

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 evaluation only addresses the functions that provide for the security of the TOE itself.

3.1 TOE Evaluated Platforms

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

3.2 TOE Architecture

The Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches 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 9300/9300L/9400/9500/9600 Series Switches are single-device security and switching solutions for protecting the network.

3.3 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 17.9. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the *Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches CC Configuration Guide* document and is downloadable from the web site:

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#

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 9300/9300L/9400/9500/9600 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.

Auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections
- creation and update of Secure Association Key
- modifications to the group of users that are part of the Authorized Administrator roles
- all use of the user identification mechanism
- any use of the authentication mechanism
- Administrator lockout due to excessive authentication failures

- any change in the configuration of the TOE
- changes to time
- initiation of TOE update
- indication of completion of TSF self-test
- maximum sessions being exceeded
- termination of a remote session
- attempts to unlock a termination session
- initiation and termination of a trusted channel

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 audit logs can be viewed on the TOE using the appropriate IOS-XE 17.9 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 cryptographic functions to implement IPsec, SSH, 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 leverages the IOS Common Cryptographic Module (IC2M), firmware version Rel5a (CAVP cert. #A1462). The IOS software calls the IC2M Rel5a cryptographic module that is validated for conformance to the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 1.

The TOE supports MACsec using the proprietary Unified Access Data Plane (UADP) Application-Specific Integrated Circuit (ASIC) (CAVP Cert. #4769). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms.

The TOE provides cryptographic support for IPsec, which is used to secure sessions between the TOE and remote syslog servers and also between the TOE and remote authentication servers (RADIUS).

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.

4.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device 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 between 8 and 16 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 supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI. The connection to the remote authentication server is secured using IPsec.

The TOE also provides authentication failure management 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 account will not be granted access until the time period has elapsed.

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 cryptographic functionality of the TOE
- 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 behavior 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 2.2e, 23 March 2020 (NDcPP22e)
- Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016 (MACsecEP12)

That information has not been reproduced here and the NDcPP22e/MACsecEP12 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/MACsecEP12 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 Extended 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 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/MACsecEP12 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 9300/9300L/9400/9500/9600 Series Switches CC Configuration Guide, Version 0.4, July 17, 2023
Cisco Catalyst 9300 Switches Hardware Installation Guide, 2023-02-14
Cisco Catalyst 9400 Switches Hardware Installation Guide, 2022-06-24
Cisco Catalyst 9500 Switches Hardware Installation Guide, 2022-09-29
Cisco Catalyst 9600 Switches Hardware Installation Guide, 2023-02-10
Release Notes for Cisco Catalyst 9300 Series Switches, 2020-03-29
Release Notes for Cisco Catalyst 9400 Series Switches, 2022-06-09
Release Notes for Cisco Catalyst 9500 Series Switches, 2023-03-10
Release Notes for Cisco Catalyst 9600 Series Switches, 2023-02-03
Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9300 Switches), 2022-08-01
Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9400 Switches), 2022-08-01
Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9500 Switches), 2022-08-01
Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9600 Switches), 2022-07-29
Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches), 2023-06-23
Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9400 Switches), 2023-06-23
Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches), 2023-06-23
Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9600 Switches), 2023-06-23
Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches), 2023-05-08
Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9400 Switches), 2023-05-08
Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches), 2023-05-08
Cisco IOS Configuration Fundamentals Command Reference, April 2010
System Message Guide for Cisco IOS XE Cupertino 17.9.x, April 14, 2023
Troubleshoot MACSEC on Catalyst 9000, Updated: July 8, 2022

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.

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 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9, Version 0.2, July 17, 2023 (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/MACsecEP12 including the tests associated with optional requirements. The AAR, in sections 1.1 and 3.4 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration consists of the following series and models:

TOE Reference	Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches
TOE Catalyst 9300 Hardware Models	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
TOE Catalyst 9300L Hardware Models	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
TOE 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
TOE Catalyst 9500 Hardware Models	C9500-12Q, C9500-24Q, C9500-40X, C9500-16X, C9500-32C C9500-32QC, C9500-24Y4C, C9500-48Y4C **With the following network modules:** C9500-NM-8X, C9500-NM-2Q

TOE 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
TOE Software Version	IOS-XE 17.9

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 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/MACsecEP12.

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 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 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.

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/MACsecEP12 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.

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 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.

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 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.

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/MACsecEP12 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.

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.

On June 30, 2023, 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/) 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", "Radius", "IOS-XE 17.9", "Cisco IOS XE 17.9", "Intel Xeon D-1523N", "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.

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 suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Assumptions and Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target, 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.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.5, July 17, 2023*.

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] Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016 (MACsecEP12).

[6] Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.5, July 17, 2023 (ST).

[7] Assurance Activity Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9, Version 0.2, July 17, 2023 (AAR).

[8] Detailed Test Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9, Version 0.2, July 17, 2023 (DTR).

[9] Evaluation Technical Report for Cisco Catalyst 9300/9300L/9400/9500/9600 Series Switches running IOS-XE 17.9, Version 0.2, July 17, 2023 (ETR)