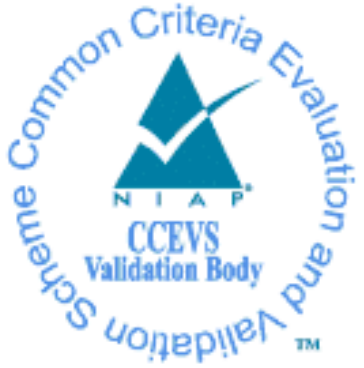
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9

Report Number: CCEVS-VR-VID11393-2023

Dated: 12/01/2023

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

Lauren Brandt
Lisa Mitchell
Linda Morrison
Clare Parran
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Khai Van
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 2
2 Identification 3
3 Assumptions & Clarification of Scope 5
4 Architectural Information 6
4.1 TOE Evaluated Configuration 6
4.2 TOE Architecture 7
4.3 Physical Boundaries 7
5 Security Policy 8
5.1 Security audit 8
5.2 Cryptographic support 8
5.3 Identification and authentication 9
5.4 Security management 10
5.5 Protection of the TSF 11
5.6 TOE access 11
5.7 Trusted path/channels 11
6 Documentation 12
7 Evaluated Configuration 14
8 IT Product Testing 15
8.1 Developer Testing 15
8.2 Evaluation Team Independent Testing 15
9 Results of the Evaluation 16
9.1 Evaluation of the Security Target (ASE) 16
9.2 Evaluation of the Development (ADV) 16
9.3 Evaluation of the Guidance Documents (AGD) 16
9.4 Evaluation of the Life Cycle Support Activities (ALC) 17
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 17
9.6 Vulnerability Assessment Activity (VAN) 17
9.7 Summary of Evaluation Results 18
10 Validator Comments/Recommendations 19
11 Annexes 20
12 Security Target 21
13 Glossary 22
14 Bibliography 23

List of Tables

Table 1: Evaluation Identifiers 4
Table 2: TOE Hardware Models 14

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Cisco Catalyst 9200CX/9300X/9300LM/9500X 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 Catonsville, MD, United States of America, and was completed in December 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)
- Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, May 10, 2016 (MACSECEP12).

The Target of Evaluation (TOE) is the Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9. The 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 ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). 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 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.9, 11/29/2023 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9
Protection Profile	(Specific models identified in Section 7)
	• collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
	• Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, May 10, 2016 (MACSECEP12)
ST	Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.9, 11/29/2023
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9, Version 0.3, 11/29/2023
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.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Lauren Brandt, Lisa Mitchell, Linda Morrison, Clare Parran, Chris Thorpe

Table 1: Evaluation Identifiers

3 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)
- Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, May 10, 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 Protection Profile for Network Devices, Extended Package MACsec Ethernet Encryption 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.
- 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.

4 Architectural Information

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

The TOE consists of a physical device, switch, and the Cisco IOS-XE 17.9 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 internet working device and forwarded to their configured destination.

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 Catalyst 9200CX/9300X/9300LM/9500X 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.

4.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 7 below.

4.2 TOE Architecture

The Cisco Catalyst 9200CX/9300X/9300LM/9500X 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 TOE is a network device that includes MACsec encryption as defined in NDcPP v2.2e and MACsec EP v1.2. The TOE is comprised of both hardware and software. The hardware is the Catalyst 9200CX, Catalyst 9300X, Catalyst 9800LM, and Catalyst 9500X switches. The software is the Cisco IOS-XE 17.9.

The Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches are single-device security and switching solutions for protecting the network.

4.3 Physical Boundaries

The TOE is a hardware and software solution that makes up the switch models as follows: Catalyst 9200CX/9300X/9300LM/9500X 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 Catalyst 9200CX/9300X/9300LM/9500X Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the https://software.cisco.com/software/csws/ws/platform/home?locale=en_US# web site.

5 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

5.1 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 is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS 1.2 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.

5.2 Cryptographic support

The TOE provides cryptographic functions to implement TLS, 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. All cryptography is implemented using the IOS Common Cryptographic Module (IC2M) version Rel5a and CiscoSSL FOM version 7.2a cryptographic modules. IC2M applies to SSH and MACsec and CiscoSSL FOM applies to TLS 1.2. The entropy source for both IC2M and CiscoSSL cryptographic modules is model dependent as listed below:

- 9200CX: ACT2Lite (ACT2) processor
- 9300X/9300LM/9500X: Cisco TRNG Core (CTC)

With the exception of C9500X-28C8D, the TOE supports MACsec using the proprietary Unified Access Data Plane (UADP) MSC version 1.0 (CAVP Cert. #4769). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms.

The C9500X-28C8D supports MACsec using the CDR5M PHY embedded within the Cisco hardware platform. The CDR5M PHY uses the Marvell Alaska C 88X7121M MACsec engine (CAVP Cert. #A1929).

The TOE provides cryptographic support for TLS 1.2, which is used to securely transmit generated audit data to an external IT entity.

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.

5.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (TOE peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. For TLS 1.2 connections to a remote syslog server, the secure channel is established only after the TOE authenticates the remote syslog server using X.509v3 certificate-based authentication.

The TOE provides authentication services for administrative users to connect to the TOE's secure Command Line Interface (CLI) Administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 8 characters as well as mandatory password complexity rules. The TOE provides Administrator authentication against a local user database. Password-based authentication can be performed on the local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE also provides 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.

5.4 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:

- Ability to administer the TOE locally and remotely
- Ability to configure the access banner
- Ability to configure the session inactivity time before session termination or locking
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to configure the authentication failure parameters
- Generate 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
- Configure the number of failed Administrator authentication attempts that will cause an account to be locked out Configure the time interval for administrator lockout due to excessive authentication failures
- Ability to modify the behaviour of the transmission of audit data to an external IT entity
- Ability to manage the cryptographic keys
- Ability to configure the cryptographic functionality
- Ability to configure thresholds for SSH rekeying
- Ability to set the time which is used for time-stamps
- Ability to configure the reference identifier for the peer
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors
- Ability to import X.509v3 certificates to the TOE's trust store
- Ability to manage the trusted public keys database

The TOE supports two separate Administrator roles: non-privileged Administrator and privileged Administrator. Only the privileged Administrator can perform the above security relevant management functions. The privileged Administrator is the Authorized

Administrator of the TOE who can enable, disable, determine, and modify the behaviour of the security functions of the TOE.

5.5 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.

5.6 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.

5.7 Trusted path/channels

The TOE allows a trusted path to be established to itself from remote Administrators over SSHv2 and initiates outbound TLS trusted channels to transmit audit messages to remote syslog servers.

The TOE supports MACsec secured trusted channels between itself and MACsec peers and TLS 1.2 between itself and a remote syslog server.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches CC Configuration Guide, Version 0.5, 11/16/2023
- The following online guides provided in PDF format:

- *Cisco Catalyst 9200 Switches Hardware Installation Guide, 2022-07-19*
- *Cisco Catalyst 9300 Switches Hardware Installation Guide, 2023-02-14*
- *Cisco Catalyst 9500 Switches Hardware Installation Guide, 2022-09-29*
- *Release Notes for Cisco Catalyst 9200 Series Switches, Cisco IOS-XE Cupertino 17.9.x, 2023-10-24*
- *Release Notes for Cisco Catalyst 9300 Series Switches, 2023-07-31*
- *Release Notes for Cisco Catalyst 9500 Series Switches, 2023-10-24*
- *Software Configuration Guide, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9200 Switches), 2022-04-09*
- *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 9500 Switches), 2022-08-01*
- *Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9200 Switches), 2022-08-01*
- *Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches), 2022-08-01*
- *Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches), 2022-08-01*
- *Command Reference, Cisco IOS-XE Cupertino 17.9.x (Catalyst 9200 Switches), 2022-07-29*
- *Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9300 Switches), 2022-07-29*
- *Command Reference, Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 Switches), 2022-08-01*
- *Cisco IOS Configuration Fundamentals Command Reference, April 2010*
- *System Message Guide for Cisco IOS XE Cupertino 17.9.x, 9-15-2023*
- *Troubleshoot MACSEC on Catalyst 9000*

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 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 Evaluated Configuration

The TOE is a hardware and software solution that makes up the switch models as follows: Catalyst 9200CX/9300X/9300LM/9500X Series Switches running Cisco IOS-XE 17.9.

Catalyst 9200CX Hardware Models	***Chassis:*** C9200CX-12T-2X2G, C9200CX-12P-2X2G, C9200CX-8P-2X2G
Catalyst 9300X Hardware Models	***Chassis:*** C9300X-48HX, C9300X-48TX, C9300X-24Y ***With the following network models*:** C9300X-NM-4C, C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y ***Chassis:*** C9300X-12Y, C9300X-48HXN, C9300X-24HX ***With the following network models*:** C9300X-NM-8M, C9300X-NM-2C, C9300X-NM-8Y
Catalyst 9300LM Hardware Models	***Chassis:*** C9300LM-24U, C9300LM-48UX, C9300LM-48T, C9300LM-48U
Catalyst 9500X Hardware Models	***Chassis:*** C9500X-28C8D
Software Version	IOS-XE 17.9

Table 2: TOE Hardware Models

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9, Version 0.3, 11/29/2023 (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP22e/MACSECEP12 including the tests associated with optional requirements.

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 9200CX/9300X/9300LM/9500X 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 9200CX/9300X/9300LM/9500X 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 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/MACSECEP12 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/MACSECEP12 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 and fuzz testing. None of the public search for vulnerabilities, or the fuzz testing uncovered any residual vulnerability.

The Evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- 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)
- CVE Database (https://www.cve.org/)
- 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 11/16/2023 with the following search terms: "TCP", "SSH", "TLS", "IC2M", "IOS Common Cryptographic Module", "CiscoSSL FOM", "Unified Access Data Plane", "UADP", "Cisco Catalyst", "IOS-XE 17.9", "Cisco IOS XE 17.9", "act2lite", "act2", "ctc", "cisco trng core", "MACsec", "MACsec Controller", "MSC", "CDR5M PHY", "catalyst 9200cx", "catalyst 9300x", "catalyst 9300lm", "catalyst 9500x", "Xilinx ZU3EG", "ARM Cortex-A53", "Intel Xeon D-1624N", "Intel Hewitt-Lake", "Cisco Silicon One Q200", "Intel Xeon D-1564N", "Intel Broadwell", "Marvell Alaska C 88X7121M".

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches CC Configuration Guide*, Version 0.5, 11/16/2023 and any additional guidance that it references. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. 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.

Note that the ST defines excluded functionality of the TOE in section 1.8. It states that excluded functionality in the evaluated configuration is a Non-FIPS 140-2 mode of operation, and the use of Telnet or Hypertext Transfer Protocol (HTTP). Additionally, administrative guidance is used to restrict the length of CKNs to 64 hex digits.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.9, 11/29/2023*.

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] Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, May 10, 2016 (MACSECEP12).

[6] Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9 Common Criteria Security Target, Version 0.9, 11/29/2023 (ST).

[7] Assurance Activity Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9, Version 0.3, 11/29/2023 (AAR).

[8] Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches CC Configuration Guide, Version 0.5, 11/16/2023 (AGD).

[9] Detailed Test Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9, Version 0.3, 11/29/2023 (DTR).

[10] Evaluation Technical Report for Cisco Catalyst 9200CX/9300X/9300LM/9500X Series Switches running IOS-XE 17.9, Version 0.3, 11/29/2023 (ETR)