National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6

Version 1.0

Report Number: CCEVS-VR-11247-2022

Dated: June 15, 2022

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

Paul Bicknell
Jenn Dotson
Sheldon Durrant
Lisa Mitchell
Linda Morrison
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Shaunak Shah
Anthony Busciglio
Bhushan Ramchandra Gosavi
Minal Prashant Wankhede
Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validation team assessment of the evaluation of the Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was completed by Acumen Security Common Criteria Testing Laboratory (CCTL) in June 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Acumen Security. 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 (NDcPP)*, Version 2.2e, March 23, 2020, and *Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP)*, Version 1.2, May 10, 2016.

The TOE is the Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 (CCEVS) 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Security Target*, version 0.12, May 31, 2022 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 (PP) 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/9500 Series Switches running IOS-XE 17.6
Protection Profile	*collaborative Protection Profile for Network Devices (NDcPP)*, Version 2.2e, March 23, 2020; *Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP)*, Version 1.2, May 10, 2016
Security Target	*Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Security Target*, Version 0.12, May 31, 2022
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6, Version 1.3, May 31, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Paul Bicknell, Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Linda Morrison, Chris Thorpe

3 Architectural Information

The TOE is the Cisco Catalyst 9300/9300L/9500 Series Switches all running Internetworking Operating System (IOS)-XE 17.6. The TOE is a purpose-built, switching and routing platform with Open System Interconnection (OSI) Layer2 and Layer3 traffic filtering capabilities. The TOE also supports Media Access Control Security (MACsec) encryption for switch-to-switch (inter-network device) security.

3.1 Evaluated Configuration

The TOE consists of a physical device, as defined in Table 3 of the ST, and the Cisco IOS-XE 17.6 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.

In addition, if the Catalyst 9300/9300L/9500 Series Switches are to be remotely administered, then the management workstation must be connected to an internal network. SSHv2 is used to securely connect to the switch. A syslog server is used to store audit records, where IPsec is used to secure the transmission of the records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic. The internal (trusted) network is in a controlled environment where implementation of security policies can be enforced.

3.2 Excluded Functionality

Functionality listed is excluded from the evaluated configuration. The exclusion of this functionality does not affect compliance to the NDcPP or MACsecEP.

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
Transport Layer Security (TLS)	TLS is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
Hypertext Transfer Protocol (HTTP)	HTTP Is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.

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

3.3 Physical Boundaries

The TOE is a hardware and software solution. The network, on which the TOE resides, 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/9500 Series Switches running IOS-XE 17.6 Common Criteria Configuration Guide*, Version 0.7, 31 May 2022 and is downloadable from the http://cisco.com web site.

4 Security Policy

The TOE is comprised of the following security features:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all Request for Comments (RFCs) of the NDcPP v2.2e and MACsec EP v1.2 as necessary to satisfy testing/assurance measures prescribed therein.

Security Audit

The Cisco Catalyst 9300/9300L/9500 Series Switches provides 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 17.6 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.

Cryptographic Support

The TOE provides cryptography in support of TOE security functionality. All the algorithms claimed have Cryptographic Algorithm Validation Program (CAVP) certificates running on the processors specified in the ST. The TOE leverages the IOS Common Cryptographic Module (IC2M), firmware version Rel5.

The TOE leverages the Firmware Image Signing module to perform the Firmware Integrity Check. The bootloader calls the Firmware Image Signing module at startup to perform a signature verification on the module firmware. The TOE supports MACsec using the proprietary Unified Access Data Plane (UADP) Application-Specific Integrated Circuit (ASIC). 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 the session between the TOE and the authentication servers. 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.

Identification and Authentication

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

The TOE provides authentication services for administrative users to connect to the TOE's secure Command Line Interface (CLI) administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE 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 an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of failed authentication attempts has exceeded the configured allowable attempts, the user is locked out until an Authorized Administrator can reenable the user account.

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

Security Management

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

- Administration of the TOE locally and remotely
- Configuration of warning and consent access banners
- Configuration of session inactivity thresholds
- Updates of the TOE software
- Configuration of authentication failures
- Configuration of the audit functions of the TOE
- Configuration of the TOE provided services
- Configuration of the cryptographic functionality of the TOE
- Generate, install, and manage Pre-Shared Keys (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.

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.

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.

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

5.1 Assumptions

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

- *collaborative Protection Profile for Network Devices (NDcPP),* Version 2.2e, March 23, 2020
- *Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP),* Version 1.2, May 10, 2016

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

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP/MACSecEP as described for this TOE in the ST. 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. Excluded functionality is identified in Section 1.8 of the ST.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices (NDcPP), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP).
- This evaluation covers only the specific device models and software as identified in the ST, and not any earlier or later versions released or in process.
- Apart from the Admin Guide identified in Section 6, additional customer documentation for the specific Switch model was not included in the scope of the evaluation and therefore 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 NDcPP/MACSecEP 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 provided by the vendor with the TOE for evaluation:

- *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Security Target*, version 0.12, May 31, 2022
- *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Configuration Guide*, Version 0.7, 31 May 2022

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 Test Plans for Cisco Catalyst 9300 and 9300L, which are not publicly available. The *Assurance Activities Report for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6*, Version 1.2, 31 May 2022 (AAR), provides an overview of testing and the prescribed assurance activities.

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 the vendor-provided guidance documentation and ran the tests specified in the NDcPP/MACSecEP. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

All testing was carried at the Acumen Security office located in Rockville, MD. The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was completed by the Acumen evaluation team.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Reports (DTR) and the ETR. The reader of this document can assume that all 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/9500 Series Switches running IOS-XE 17.6 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the Evaluation team performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP).

8.1 Evaluation of Security Target

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/9500 Series Switches running IOS-XE 17.6 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.

8.2 Evaluation of Development Documentation

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 ST's TOE Summary Specification (TSS). Additionally, the evaluator performed the Assurance Activities specified in the collaborative NDcPP/MACSecEP 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.

8.3 Evaluation of Guidance Documents

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.

8.4 Evaluation of Life Cycle Support Activities

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.

8.5 Evaluation of Test Documentation and the Test Activity

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP/MACSecEP and recorded the results in the proprietary DTR, 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.

8.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Vulnerability Assessment for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6*, Version 1.2, May 31, 2022, report prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on May 31, 2022, did not uncover any residual vulnerability.

The Evaluation team searched:

- www.cisco.com
- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/
- https://www.cvedetails.com/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com

- https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- Cisco Switch
- Cisco IOS XE 17.6
- Catalyst Switch
- Catalyst 9300
- 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
- C9300-NM-4G
- C9300-NM-8X
- C9300-NM-2Q
- C9300-NM-4M
- C9300-NM-2Y
- Catalyst 9300L
- C9300L-24T-4G
- C9300L-48T-4G
- C9300L-24P-4G
- C9300L-48P-4G
- C9300L-24T-4X
- C9300L-48T-4X
- C9300L-24P-4X
- C9300L-48P-4X
- C9300L-48PF-4G
- C9300L-48PF-4X
- C9300L-24UXG-4X
- C9300L-24UXG-2Q
- C9300L-48UXG-4X
- C9300L-48UXG-2Q
- Catalyst 9500
- C9500-12Q
- C9500-24Q

- C9500-40X
- C9500-16X
- C9500-32C
- C9500-32QC
- C9500-24Y4C
- C9500-48Y4C
- C9500-NM-8X
- C9500-NM-2Q
- Intel Broadwell processor
- Intel Goldmont processor
- Intel Xeon D-1523N
- Intel Atom C3558
- Intel Xeon D-1526
- UADP MSC
- Unified Access Data Plane (UADP)
- IOS XE IPSec
- IOS XE SSH
- IOS XE VPN
- IOS XE MACsec
- IC2M
- IOS Common Cryptographic Module
- TCP
- UDP

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.

8.7 Summary of Evaluation Results

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

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

9 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Configuration Guide*, Version 0.7, 31 May 2022. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. 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.

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. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later were evaluated.

10 Annexes

Not applicable.

11 Security Target

Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Security Target, version 0.12, May 31, 2022

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

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

1. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, April 2017.
2. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
3. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5, April 2017.
5. *collaborative Protection Profile for Network Devices (NDcPP)*, Version 2.2e, March 23, 2020.
6. *Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP)*, Version 1.2, May 10, 2016
7. *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Security Target*, Version 0.12, May 31, 2022.
8. *Evaluation Technical Report for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6*, Version 1.3, May 31, 2022.
9. *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Configuration Guide*, Version 0.7, 31 May 2022.
10. *Vulnerability Assessment for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6*, Version 1.2, May 31, 2022.
11. *Assurance Activity Report for Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6*, Version 1.2, May 31, 2022
12. *Test Plan for Cisco Catalyst 9300*, Version 1.2, May 31, 2022.
13. *Test Plan for Cisco Catalyst 9300L*, Version 1.2, May 31, 2022.