National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9, Version 1.0

Report Number: CCEVS-VR-VID10940-2019

Dated: March 14, 2019

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior
Jenn Dotson
Sheldon Durrant
Linda Morrison
The MITRE Corporation

Common Criteria Testing Laboratory

Kenneth Lasoski
Zalman Kuperman
Kevin Zhang
Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the Security Target (ST).

The evaluation was completed by Acumen Security in March 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, 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 defined in the U.S. Government *collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018* (NDcPP20E) and *NDcPP Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016* (MACsec EP).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP20E. 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The Validation Team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Security Target, Version 1.0, 5 March 2019* 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 CCTLs. CCTLs evaluate products against Protection Profile(s) (PP) containing Assurance Activities (AA), which are interpretation of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP and in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance 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 PPs 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 3650 and 3850 Series Switches running IOS-XE 16.9
Protection Profile	NDcPP 2.0e and MACsec EP 1.2
Security Target	Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Security Target, Version 1.0, 5 March 2019
Evaluation Technical Report	Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Evaluation Technical Report, Version 1.2, March 2019
CC Version	Version 3.1, Revision 4
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 Linda Morrison

3 Architectural Information

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

The TOE is a hardware and software solution that makes up the switch models as follows: Catalyst 3650 and 3850 Series Switches running Cisco IOS-XE 16.9. They are switching and routing platforms that provide connectivity and security services, including MACsec encryption in a single device. The network, on which they reside, is considered part of the environment.

Catalyst 3650 and 3850 Series Switches primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation.
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program).
- USB port (v2.0) (note, none of the USB devices are included in the TOE).
    - Type A for Storage, all Cisco supported USB flash drives.
    - Type mini-B as console port in the front.
- 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.
- Management is through a 10/100/1000 Ethernet port or an RJ-45 console port
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

3.1 TOE Evaluated Platforms

The evaluated platforms consist of the following modes:

Cisco Catalyst 3650 Series

- WS-C3650-24TS
- WS-C3650-48TS
- WS-C3650-24PS
- WS-C3650-48PS
- WS-C3650-48FS
- WS-C3650-24TD
- WS-C3650-48TD
- WS-C3650-24PD
- WS-C3650-48PD
- WS-C3650-48FD
- WS-C3650-48TQ
- WS-C3650-48PQ
- WS-C3650-48FQ)

- WS-C3650-48FQM

Cisco Catalyst 3850 Series

- WS-C3850-24T
- WS-C3850-48T
- WS-C3850-24P
- WS-C3850-48P
- WS-C3850-48F
- WS-C3850-24U
- WS-C3850-48U
- WS-C3850-12S
- WS-C3850-24S
- WS-C3850-12XS
- WS-C3850-24XS
- WS-C3850-24XU
- WS-C3850-48XS

3.2 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

3.3 Physical Boundaries

The TOE is comprised of the physical specifications as described in the ST. The hardware, size and the interfaces are based on the number of ports on a particular model. For example the 3650, WS-C3650-24TS measures 1.73 x 17.5 x 19.125 and has 24 ports (10M/100M/1000M (10 Gigabit Ethernet SFP+ Ports and Gigabit Ethernet SFP Ports). The USB, RJ-45, StackWise, power, software and processors are the same on all hardware series listed.

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- 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 RFCs of the NDcPP v2.0e and MACsec EP v1.2 as necessary to satisfy testing/assurance measures prescribed therein.

4.1 Security Audit

The Cisco Catalyst 3650 and 3850 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; and
- 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 can be configured to block new permit actions.

The audit logs can be viewed on the TOE using the appropriate IOS 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 cryptography in support of TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment - Cavium Octeon CN6230, a MIPS64 processor).

The TOE leverages the IOS Common Criteria Module (IC2M) Rel5 as identified in the table below. The IOS software calls the IC2M Rel5 (Firmware Version: Rel 5) certificate 2388 and has been validated for conformance to the requirements of FIPS 140-2 Level 1.

In addition, the TOE supports MACsec using proprietary Unified Access Data Plane (UADP) ASIC. The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms.

Refer to Table 1 for algorithm certificate references.

Table 1 FIPS References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	AES Key Wrap in CMAC, CBC and GCM (128 and 256 bits)	4583	IC2M	FCS_COP.1/DataEncryption
			4769	UADP MSC	
SHS (SHA-1, SHA-256 and SHA-512)	Cryptographic hashing services	Byte Oriented	3760	IC2M	FCS_COP.1/Hash

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	3034	IC2M	FCS_COP.1/KeydHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	1529	IC2M	FCS_RBG_EXT.1
RSA	Key Generation and Signature Verification	FIPS PUB 186-4 Key Generation PKCS #1 v2.1 2048 bit key	2500	IC2M	FCS_CKM.1 FCS_COP.1/SigGen

The TOE provides cryptography in support of VPN connections that includes remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

The cryptographic services provided by the TOE are described in Table 2 below.

Table 2 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic. Used to encrypt MACsec traffic.
HMAC	Used for keyed hash, integrity services in IPsec and SSH session establishment.
DH	Used as the Key exchange method for SSH and IPsec
Internet Key Exchange	Used to establish initial IPsec session.

Cryptographic Method	Use within the TOE
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services Used in Cryptographic Key Generation and Key Establishment
Secure Shell Establishment	Used to establish initial SSH session.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
SP 800-90 RBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in IPsec session establishment. Used in SSH session establishment Used in MACsec session establishment

The Cisco Catalyst 3650 and 3850 Series Switches platforms contain the following processors as listed in Table 3.

Table 3 Catalyst 3650 and 3850 Series Switches Platform Processors

Chassis	CPU Designation
3650	Cavium Octeon CN6230, a MIPS64 processor
3850	Cavium Octeon CN6230, a MIPS64 processor

4.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN 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 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 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 TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded the configured allowable attempts, the user is locked out until an Authorized Administrator can enable the user account.

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 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 PSK;
- Manage the Key Server, CAK and MKA participants; and
- 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 has the ability to enable, disable, determine and modify the behavior of all 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 is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS functions.

The TOE is able to verify any software updates prior to the software updates being installed

on the TOE to avoid the installation of unauthorized software.

The TOE is also able to detect replay of information received via secure channels (MACsec). The detection 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 are 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 be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an Authorized Administrator can enable the user account.

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

The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect the communications with the CA server.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed below are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

Threat	Threat Definition
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY	An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient.
T.NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization.
T.UNTRUSTED_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.

5.3 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 level of assurance for this evaluation is defined within the NDcPP 2.0e and MACsec EP 1.2.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- 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.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Security Target, Version 1.0, 5 March 2019
- Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, 27 November 2018

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in ETR for Cisco Catalyst 3650 and 3850 Series Switches, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The Evaluation Team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 2.0e and MACsec EP 1.2. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

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: Detailed Test Report (DTR) and ETR. The reader of this document can assume that 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 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Catalyst 3650 and 3850 Series Switches to be Part 2 extended and meets the assurance requirements contained in the PP. Additionally, the evaluator performed the AAs specified in the NDcPP 2.0e and MACsec EP.

8.1 Evaluation of Security Target (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst 3650 and 3850 Series Switches that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP 2.0e and MACsec EP 1.2.

8.2 Evaluation of Development Documentation (ADV)

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. Additionally, the evaluator performed the AAs specified in the NDcPP 2.0e and MACsec EP 1.2 related to the examination of the information contained in the TOE Summary Specification.

8.3 Evaluation of Guidance Documents (AGD)

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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the AAs specified in the NDcPP 2.0e and MACsec EP 1.2 related to the examination of the information contained in the operational guidance documents.

8.4 Evaluation of Life Cycle Support Activities (ALC)

The Evaluation Team found that the TOE was identified.

8.5 Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation Team ran the set of tests specified by the AAs in the NDcPP 1.0 and MACsec EP 1.2 and recorded the results in a Test Report, summarized in the ETR and AAR.

8.6 Vulnerability Assessment Activity (VAN)

The Evaluation Team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 test activities 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 performed the AAs in the NDcPP 2.0e and MACsec EP 1.2, and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

The Validation Team suggests that the consumer pay particular attention to the evaluated configuration of the products(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST, and only the functionality implemented by the SFR's within the ST was evaluated. All other functionality provided by the product(s), to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about the effectiveness of the additional functionality.

Consumers employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

10 Annexes

Not applicable.

11 Security Target

The ST is identified as: *Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Security Target, Version 1.0*, 5 March 2019

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E)
6. NDcPP Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016 (MACsec EP).
7. Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Security Target, Version 1.0, 5 March 2019
8. Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9 Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, 27 November 2018
9. Assurance Activity Report for Cisco Catalyst 3650 and 3850 Series Switches running on IOS-XE 16.9, Version 1.2, 31 January 2019
10. Test Plan for Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9, Version 1.0, Date 1/31/2019 (NDcPP)
11. Test Plan for Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.9, Version 1.1, Date 12/20/2018 (MACsec)