National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3

Report Number:	CCEVS-VR-VID11177-2021
Dated:	08/29/2021
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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome F. Myers, PhD
Marybeth S. Panock

Common Criteria Testing Laboratory

Cody Cummins
Shahid Islam
Gossamer Security Solutions
Columbia, MD

Table of Contents

1 Executive Summary

The evaluation of Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches was performed by Gossamer Security Solutions, in Columbia, MD and was completed in August 2021. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Gossamer Security Solutions determined that the product satisfies evaluation assurance level "EAL 1" as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the *Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 Common Criteria Security Target, Version 1.0, 3 August 2021.*

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 evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of Cisco Catalyst IE3200, IE3300, IE3400, IE3400H Series Switches running IOS-XE 17 by any agency of the US Government and no warranty of the product is either expressed or implied. This Validation Report applies only to the specific version of the TOE as evaluated.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the Evaluation Technical Report (ETR) and the Assurance Activities Report (AAR). 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). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Gossamer evaluation team determined that the product meets the Common Criteria requirements of the collaborative Protection Profile for Network Devices Version 2.2e, 23-March-2020. The technical information included in this report was obtained from the "Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 Common Criteria Security Target" Version 1.0, 3 August 2021 and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020
ST	Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 Common Criteria Security Target, Version 1.0, 3 August 2021
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3, version 0.1, 08/28/2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jerome F. Myers, PhD Marybeth S. Panock

3 Architectural Information

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

The Target of Evaluation (TOE) is the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches. The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities.

3.1 TOE Evaluated Configuration

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

3.2 TOE Architecture

The TOE is a hardware and software solution that makes up the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switch models as follows: IE3200, IE3300, IE3400 and IE3400H running Cisco IOS-XE 17.3. 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 Cisco Catalyst Industrial Ethernet IE3x00 Rugged 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. An external 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, one that is in a controlled environment where implementation of security policies can be enforced.

The following figure provides a visual depiction of an example TOE deployment.

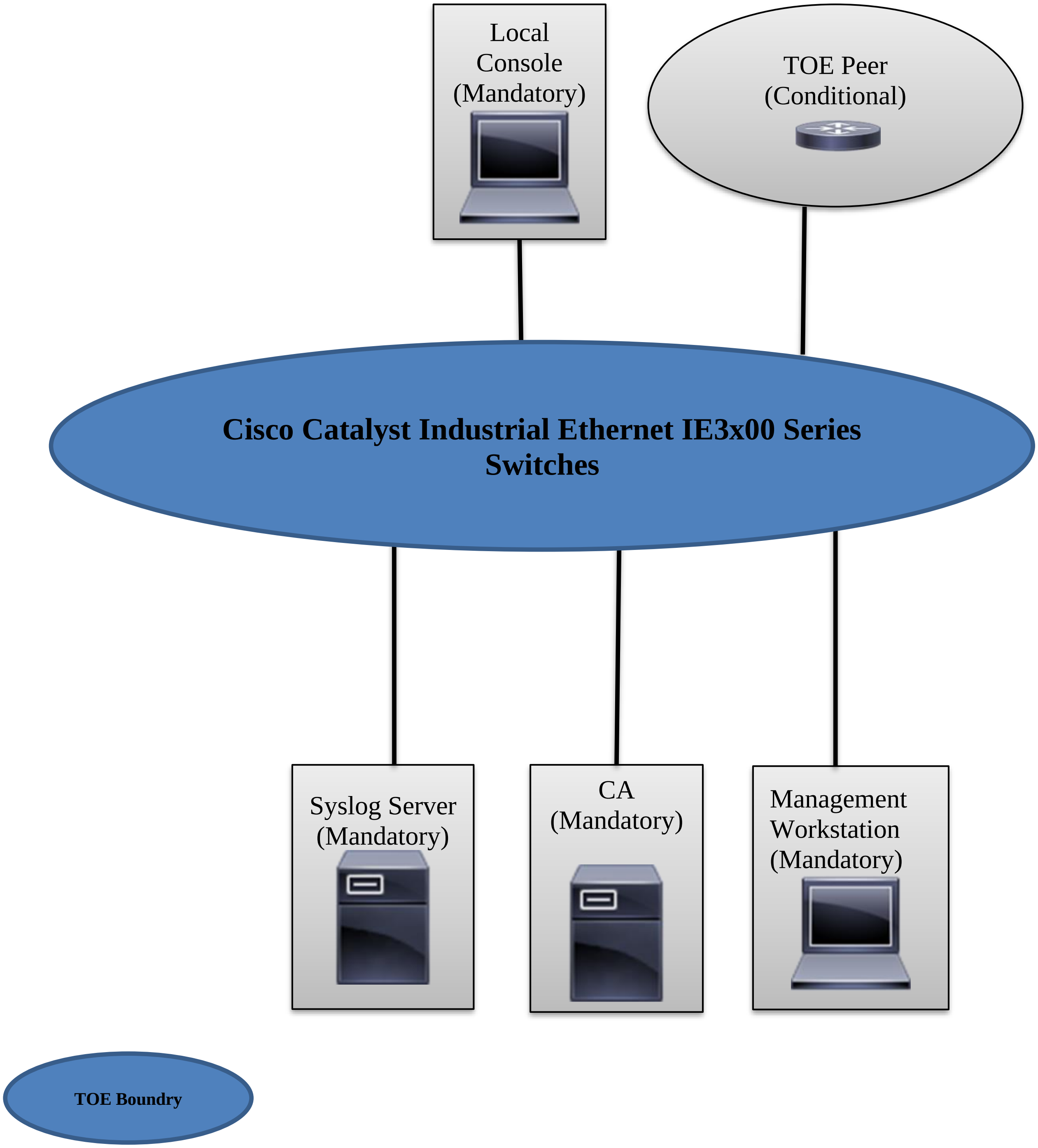
Local Console (Mandatory)
TOE Peer (Conditional)
Cisco Catalyst Industrial Ethernet IE3x00 Series Switches
Syslog Server (Mandatory)
CA (Mandatory)
Management Workstation (Mandatory)
TOE Boundry

Figure 1 TOE Example Deployment

The previous figure includes the following devices, noting the TOE is only the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches and only one TOE device is required for the deployment of the TOE in the evaluated configuration.

- Identifies the TOE Models
  - Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running Cisco IOS-XE 17.3
- Identifies the following IT entities that are considered to be in the IT Environment:
  - Syslog (audit) Server with a secure connection using IPsec
  - Local Console to support local Administration (direct connection)
  - Management Workstation to support remote Administration with a secure connection using SSHv2 Client
  - Certificate Authority (CA) for X509 certificate validation with a secure connection using IPsec
  - TOE Peer (Conditional) with a secure connection using IPsec

3.3 Physical Boundaries

The TOE is a hardware and software solution that makes up the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switch models as follows: IE3200, IE3300, IE3400 and IE3400H running Cisco IOS-XE 17.3. The network, on which they reside is considered part of the operational environment. The TOE deployment and operational guidance documentation that is considered to be part of the TOE can be found in the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and is downloadable from the http://cisco.com web site. The TOE is comprised of the following physical specifications as described in Table 1 below. The hardware, size and the interfaces are based on the number of ports.

Table 1 Hardware Models and Specifications

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst Industrial Ethernet Series IE3200 Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8lbs	Supports up to 8 PoE/PoE+ ports [Power budget - 240W]	8 -10/100/1000 RJ45 Copper ports, 2 - 100/1000 SFP Ports, 1 RS-232 (via RJ-45), 1 USB Mini Type B
Cisco Catalyst Industrial Ethernet Series IE3300 Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8 lbs	up to 24x PoE/PoE+ ports or 4x 802.3bt type 4 ports (with 2.5G expansion module) with the all GE PoE enabled base [Power budget - 360W] OR up to 24x PoE/PoE+ ports or 4x 802.3bt type 3 ports (on PoE base system) or 4x 802.3bt type 4 ports (with 2.5G expansion module) with the 10G PoE enabled base	8 -10/100/1000 RJ45 Copper ports, 2 - 100/1000 SFP Ports, 4 1GE/2.5G RJ45 Copper ports 2 1GE/10G SFP+ ports 1 RS-232 (via RJ-45), 1 USB Mini Type B

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst Industrial Ethernet IE3400 Series Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8 lbs to 6 in. X 4.4 in. X 5.3 in. 5.0 lbs	Supports up to 24 PoE/PoE+ ports or up to 8 PoE/PoE+ Ports and 4 “802.3bt type 4” Ports with the 2.5G expansion module 2 [System Power budget - 480W]	8 up to 1610/100/1000 RJ45 Copper ports, 2 up t0 8 100/1000 SFP Ports, 4 1GE/2.5G RJ45 Copper Ports
Cisco Catalyst Industrial Ethernet IE3400H Series Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		9.58 x 7.90 x 3.15 in. 8.45 lbs to 9.58 x 10.90 x 3.15 in.	IP67-rated PoE DC-DC power supply, Input:18V-60V Output: 54V, 3.1A max 160W OR IP67-rated PoE AC-DC power supply, input 85-264VAC/88-300VDC, Output 54V, 3.1A max, 180Watts	8 up to 24 - 10/100 Fast Ethernet ports, 8 up to 24 - 10/100/1000 Gigabit Ethernet ports

4 Security Policy

The TOE enforces the following security policies as described in the ST:

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

4.1 Security Audit

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged 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.

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 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 other TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment – Xilinx ZU3EG processors).

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

The TOE provides cryptography in support of secure 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.

4.3 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. 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 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 local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys.

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.

4.4 Security Management

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

- Administration of the TOE locally and remotely;
- Configuration of warning and consent access banners;
- Configuration of session inactivity thresholds;
- Updates of the TOE software;
- Configuration of authentication failures;
- Configuration of the audit functions of the TOE;
- Configuration of the TOE provided services;
- Configuration of the cryptographic functionality of the TOE.

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 and 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-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 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 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 Authorized Administrator to re-authenticate to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the "exit" command.

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 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 to protect the communications with the CA server.

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 (NDcPP22e)

That information has not been reproduced here and the NDcPP22e 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 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.

6 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 Protection Profile for Network Devices 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 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the functionality listed in Table 8 Section 9.1 is excluded from the scope of the evaluation.

7 Documentation

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

- Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE340H Series) Switches running IOS-XE 17.3 Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, 27 May 2021

Only this manual only this manual and sections of other manuals explicitly referenced by it should be trusted for the configuration, administration, and use of the product in its evaluated configuration.

8 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 Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3, Version 0.1, 08/28/2021 (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 purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the collaborative Protection Profile for Network Devices Version 2.2e, 23-March-2020 [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the collaborative Protection Profile for Network Devices Version 2.2e and the Evaluation Activities for Network Device cPP Version 2.2. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Gossamer CCTL facilities in Columbia, Maryland. Testing occurred from November 2020 and was completed in August 2021.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the vendor-provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. The Independent Testing activity is documented in the Assurance Activities Report (AAR), which is publicly available, and is not duplicated here. A description of the test configurations and the test tools may be found in Section (y) of that report.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for collaborative Protection Profile for Network Devices Version 2.2e were fulfilled.

8.3 Test Configuration

The evaluation team established a test configuration comprising:

TOE Platforms:

- IE3200

Supporting Products:

- Test Server
  - Audit Server - Ubuntu 16.04 audit server
    - Rsyslog v8.16.0
  - VPN Client - Strongswan 5.3.5
  - SSH Client – OpenSSH 7.2p2
- Management PC – Windows 10 Enterprise (with Wireshark and Putty installed)

9 TOE Evaluated Configuration

9.1 Evaluated Configuration

The TOE is comprised of both software and hardware. The hardware is comprised of the following hardware models IE3200, IE3300, IE3400 and IE3400H. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.3. The evaluated configuration is comprised of this hardware and software as configured in accordance with the documentation identified in Section 7.

9.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 2 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
SNMP: The Simple Network Management Protocol is an application layer protocol, facilitates the exchange of management information among network devices	SNMP is not associated with Security Functional Requirements claimed in [NDcPP].

Excluded Functionality	Exclusion Rationale
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.
TLS Transport layer Security	TLS is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
SSL Secure Socket Layer	SSL is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
HTTP Hypertext Transfer Protocol	Hypertext Transfer Protocol is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.
HHTPS Hypertext Transfer Protocol Secure	Hypertext Transfer Protocol Secure is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.
AH Authentication Header (part of IPsec)	Encapsulating Security Payload (part of IPsec) must be used in all IPsec connections.

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The (AGD) Table 14 provides a list of the services and protocols allowed in the evaluated configuration.

The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.2e.

10 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 Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

10.1 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 Industrial Ethernet 3x00 Rugged Series

(IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

10.2 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 related to the examination of the information contained in the TSS.

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

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

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

10.5 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 and recorded the results in a Test Report, summarized in the AAR.

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

10.6 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. Neither the public search for vulnerabilities nor 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)
- Exploit / Vulnerability Search Engin (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- 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 08/28/2021 with the following search terms: "Cisco IOS XE", "Cisco Catalyst", "IE3200 ", "IE3300 ", "IE3400", "IE3400H", "Xilinx ZU3EG", "IOS Common Cryptographic Module ", "IC2M".

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

10.7 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.

11 Validator Comments/Recommendations

The validators recommend that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

12 Security Target

The Security Target is identified as: Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE340H) Switches running IOS-XE 17.3 Common Criteria Security Target, Version 1.0, 3 August 2021.

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, 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 Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 (NDcPP22e)

[6] Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 Common Criteria Security Target, Version 1.0, 3 August 2021.

[7] Assurance Activity Report for Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3, Version 0.1, 08/28/2021 (AAR).

[8] Detailed Test Report for Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3, Version 0.1, 08/28/2021 (DTR).

[9] Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3, Version 0.1, 08/28/2021 (ETR).