National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12

Report Number: CCEVS-VR-VID11443-2024
Dated: 05/15/2024
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

Viet Hung Le
Patrick Mallett
Jerome Myers
Dave Thompson

The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Julia Miller
Katie Sykes

Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in May 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the

> collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

The Target of Evaluation (TOE) is the Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 Common Criteria Security Target, Version 0.7, 05/15/2024 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 Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 (Specific models identified in Section 8)
Protection Profile	• collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
ST	Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 Common Criteria Security Target, Version 0.7, 05/15/2024
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12, Version 0.2, 05/15/2024
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.

Item	Identifier
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Viet Hung Le, Patrick Mallett, Jerome Myers, and Dave Thompson of the Aerospace Corporation.

3 Architectural Information

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

The Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches, running IOS-XE 17.12, is a purpose-built switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities.

The TOE is comprised of both software and hardware. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.12. The hardware models that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged 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;
- x86 CPU complex with minimum, based on model of 2 GB memory, 1.5 GB of flash;
- Flash memory (EEPROM), used to store the Cisco IOS-XE image (binary program);
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs and
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (for example, 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;
- Dedicated management port on the switch, RJ-45 console port and a USB mini-Type B console connection;
- Built for harsh environments and temperature ranges, fanless, convection-cooled with no moving parts for extended durability and hardened for vibration, shock and surge, and electrical noise immunity.

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 4 below.

3.1 TOE Evaluated Configuration

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

3.2 TOE Architecture

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches are switching and routing platforms that provide connectivity and security services. These switches offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers. The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches is a single-device security and switching solutions for protecting the network.

3.3 Physical Boundaries

The TOE is a hardware and software solution that makes up the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switch models as follows: IE3200, IE3300, IE3400 and IE3400H running Cisco IOS-XE 17.12. The network, on which they reside is considered part of the operational environment.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The Cisco Catalyst 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.

Auditable events include:

- Failure on invoking cryptographic functionality such as establishment, termination, and failure of cryptographic session establishments and connections.

- Modifications to the group of users that are part of the Authorized Administrator roles.
- Use of the user identification mechanism.
- Use of the authentication mechanism.
- Unsuccessful login attempts limit is met or exceeded.
- Change in the configuration of the TOE.
- Changes to time.
- Initiation of TOE update.
- Indication of completion of TSF self-test.
- Termination of a remote or local 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[1].

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 (ARM Cortex-A53).

The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a as identified in Table 9 in Section 1.6.2 of the ST. The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5a (Firmware Version: Rel 5a) 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.

4.3 Identification and authentication

The TOE performs two types of authentications: device-level authentication of the remote device (TOE peers) and user authentication for the Authorized Administrator of the TOE.

[1] If the syslog server is unavailable long enough that the capacity of the local audit storage is exhausted, some audit records will be lost.

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 between 1-127 characters. 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 been exceeded, the user is locked out for an administrator specified time period.

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 remote administrative interface and local interface to perform security management functions. This includes the ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination as well as an ability to update TOE software. The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

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 the reading of cryptographic keys and passwords. Additionally, Cisco IOS-XE is not a general-purpose operating system. Access to Cisco IOS-XE memory space is restricted to Cisco IOS-XE functions.

The TOE can verify software updates prior to the software updates being installed on the TOE. This verification helps prevent the installation of unauthorized software.

The TOE internally maintains the date and time. This date and time are used in 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. Discontinuities of time are logged.

Finally, the TOE performs self-testing to verify correct operation of the TOE itself and of the cryptographic module.

4.6 TOE access

The TOE can terminate inactive local and remote 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 "exit" or the "logout" 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 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.

5 Assumptions & Clarification of Scope

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

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)

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.

Clarification of scope
All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Protection Profile for Network Devices 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. Specifically, as noted in Section 1.7, Table 11 of the Security Target, the use of HTTP/HTTPS or SNMP for remote management was not covered by the evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 CC Configuration Guide, Version 0.8, 05/15/2024
Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide, 12-14-2023
Command Reference, Cisco IOS XE Dublin 17.12.x (Catalyst 9300 Switches), 7-28-2023
Programmability Command Reference, Cisco IOS XE Dublin 17.12.x, 7-28-2023
Security Configuration Guide, Cisco Catalyst IE3x00 and IE3100 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches, 12-8-2023
System Message Guide for Cisco IOS XE Dublin 17.12.x, 9-21-2023

Only the guidance found in the above documents and the specific sections of other documents they reference should be trusted for the installation, administration, and use of the product in its evaluated configuration.

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 Assurance Activity Report for Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12, Version 0.2, 05/15/2024 (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. The test configuration and testing tools used are described in Section 3.4 of the Assurance Activity Report (AAR)..

8 Evaluated Configuration

The TOE is a hardware and software solution composed of the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches running IOS-XE 17.12.

The evaluated configuration consists of the following devices, when configured in accordance with the documentation identified in Section 6:

Catalyst IE3200 Hardware Models	IE-3200-8T2S, IE-3200-8P2S
Catalyst IE3300 Hardware Models	IE-3300-8T2S, IE-3300-8P2S, IE-3300- 8T2X, IE-3300- 8U2X
Catalyst IE3400 Hardware Models	IE-3400-8T2S, IE-3400-8P2S
Catalyst IE3400H Hardware Models	IE-3400H-8FT, IE-3400H-8T, IE-3400H-16FT, IE-3400H-16T, IE-3400H-24FT, IE-3400H-24T
Software Version	IOS-XE 17.12

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

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

9.3 Evaluation of the Guidance Documents (AGD)

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

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e and recorded the results in a Test Report, summarized in the AAR.

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

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. None of the public search for vulnerabilities, or the fuzz testing uncovered any residual vulnerability.

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

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
- 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 05/14/2024 with the following search terms: "Cisco IOS XE", "IOS-XE 17", "Cisco Catalyst", "IE3200", "IE3300", "IE3400", "IE3400H", "Xilinx ZU3EG", "Arm Cortex-A53", "IOS Common Cryptographic Module", "IC2M", "SSH", "IPsec", "IKE", "IC2M Rel5a".

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments/Recommendations

All validator comments and recommendations are adequately addressed in the Assumptions and Clarification of Scope section.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 Common Criteria Security Target, Version 0.7, 05/15/2024*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

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

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12 Common Criteria Security Target, Version 0.7, 05/15/2024 (ST).

[6] Assurance Activity Report (NDcPP22e) for Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12, Version 0.2, 05/15/2024 (AAR).

[7] Detailed Test Report for Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12, Version 0.2, 05/15/2024 (DTR).

[8] Evaluation Technical Report for Cisco Catalyst Industrial Ethernet 3200, 3300, 3400, 3400H (IE3x00) Rugged Series Switches running IOS-XE 17.12, Version 0.2, 05/15/2024 (ETR)