

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

for the

Cisco Catalyst 9400 Series Switches running IOS-XE 16.6

Report Number: CCEVS-VR-VID10863-2018

Dated: 04/16/2018

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

Sheldon Durrant

Paul Bicknell

Linda Morrison

Brad O'Neill

The MITRE Corporation

Common Criteria Testing Laboratory

Kevin Micciche

Furukh Siddique

Acumen Security, LLC

Table of Contents

1	Executive Summary	4
2	Identification	5
3	Architectural Information	6
4	Security Policy	7
4.1	Security Audit	7
4.2	Cryptographic Support	8
4.3	Identification and authentication	8
4.4	Security Management	9
4.5	Protection of the TSF	9
4.6	TOE Access	9
4.7	Trusted path/Channels	10
5	Assumptions, Threats & Clarification of Scope	11
5.1	Assumptions	11
5.2	Threats	11
5.3	Clarification of Scope	11
6	Documentation	12
7	TOE Evaluated Configuration	13
7.1	Evaluated Configuration	13
7.2	Excluded Functionality	15
8	IT Product Testing	16
8.1	Developer Testing	16
8.2	Evaluation Team Independent Testing	16
9	Results of the Evaluation	17
9.1	Evaluation of Security Target	17
9.2	Evaluation of Development Documentation	17
9.3	Evaluation of Guidance Documents	17
9.4	Evaluation of Life Cycle Support Activities	18
9.5	Evaluation of Test Documentation and the Test Activity	18
9.6	Vulnerability Assessment Activity	18
9.7	Summary of Evaluation Results	18
10	Validator Comments & Recommendations	20
11	Annexes	21
12	Security Target	22
13	Glossary	23
14	Bibliography	24

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This 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 ST.

The evaluation was completed by Acumen Security in January 2018. 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 Protection Profile for Security Requirements for NDcPP 2.0.

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), as interpreted by the Assurance Activities contained in the NDcPP 2.0. 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 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 the functional requirements and assurance requirements stated in the Security Target (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 evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 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(s) 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 9400 Series Switches running IOS-XE 16.6
Protection Profile	NDcPP 2.0
Security Target	Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 Security Target
Evaluation Technical Report	Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 ETR
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Paul Bicknell, Sheldon Durrant, Linda Morrison, Brad O'

3 Architectural Information

The Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 (herein after referred to as Cisco Cat 9K Series). The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities. The TOE is a switching and routing platform used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer2 switch, it performs analysis of incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. As a Layer3 switch/router, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet.

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 v2.0 as necessary to satisfy testing/assurance measures prescribed therein.

4.1 Security Audit

The Cisco Catalyst 9400 Series Switches provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity that triggered the event and the outcome of the event.

The 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;
- 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 the audit messages to an external syslog server. Communication with the syslog server is protected by 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 (delete) 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 – Intel Xeon processor). All the algorithms claimed have CAVP certificates (Operation Environment - Cavium Octeon CN6230, a MIPS64 processor).

The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) certificate 2388 and has been validated for conformance to the requirements of FIPS 140-2 Level 1.

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 TOEs 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.

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 following functionality to securely manage the TOE:

- 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; and
- 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 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-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 is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the switch 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 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 paths 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 remote 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.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

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

- Collaborative Protection Profile for Network Devices, Version 2.0, 5 May 2017 (NDcPPv2)

That information has not been reproduced here and the NDcPPv2 should be consulted if there is interest in that material.

5.2 Threats

The Security Problem Definition, including the threats, may also be found in the NDcPPv2. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP 2.0.
- Consistent with the expectations of the Protection Profile, 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. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation


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

- Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 Security Target, Version 1.0
- Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a hardware and software solution that makes up the router models as follows:

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst 9400 Series	Intel Xeon	Cisco IOS-XE 16.6		<p>C9407R is a 10RU - 17.41 x 17.30 x 16.30 in and 63.0 lb.</p> <p>C9410R is a 13RU - 22.61 x 17.30 x 16.30 in and 65.0 lb</p>	<p>There are three modes of operation supported by Cisco Catalyst 9400 power supplies. In all the modes the power supplies can be of different wattage and type whether AC or DC.</p> <p>Redundant N + N mode</p> <p>The Cisco Catalyst 9400 Chassis also supports N + N redundancy with N independent input circuits and safeguards against failure of N (+N) of the circuits as opposed to power supply unit failure.</p> <p>Redundant N + 1 mode</p> <p>The Cisco Catalyst 9400 Chassis also supports N + 1 redundancy with N independent input circuits and safeguards against failure of one (+1) of the circuits as opposed to power supply unit failure.</p> <p>Combined mode</p> <p>In this mode the power available for the entire chassis is equal to the sum of the output power of both of the power supplies multiplied by the share ratio.</p> <p>P = Power output of one power-supply unit</p> <p>Total combined mode power = P + (N-1) * P * (share ratio)</p>	<p>Both models support C9400-SUP-1 supervisor card and C9400-LC-48U (Cisco Catalyst 9400 Series 48-Port UPOE 10/100/1000 (RJ-45) and/or C9400-LC-48T (Cisco Catalyst 9400 Series 48-Port 10/100/1000 (RJ-45) line cards</p> <p>In both models:</p> <ul style="list-style-type: none"> • Slots 3 and 4 are reserved for supervisor engines only in Cisco Catalyst C9407R; slots 1-2 and 5-7 are reserved for line cards. • Slots 5 and 6 are reserved for supervisor engines only in Cisco Catalyst C9410R; slots 1-4 and 7-10 are reserved for line cards. • Linecards are not supported in the Supervisor slots

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 16.6. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image.

7.2 Excluded Functionality

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

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Catalyst 9400 Series Switches running IOS-XE 16.6, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 2.0. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (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 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 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 2.0.

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 Development Documentation

The evaluation team applied each EAL 1 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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP 2.0 related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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. The guides were assessed during the design and testing phases of

the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP 2.0 and related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP 2.0 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP 2.0, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 addressed the vulnerability analysis Assurance Activities in the NDcPP 2.0, 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 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 Assurance Activities in the NDcPP 2.0, and

correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that consumers pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed above to ensure the evaluated configuration is established and maintained.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality, including the excluded functionality discussed above, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated version of the products utilizes the *Cavium Octeon CN6230 MIPS64* processor and no earlier or later versions were evaluated and therefore cannot be considered as compliant.

The TOE stores a limited amount of audit records in its internal persistent storage. It is recommended that the administrator configure the TOE to export audit logs to a remote audit storage server.

11 Annexes

Not applicable.

12 Security Target

Cisco Catalyst 9400 Series Switches running IOS-XE 16.6 Security Target, Version 1.0

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.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.