National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cisco Nexus 9000 Series Switches Running NX-OS 10.4

Report Number:	**CCEVS-VR-VID11514-2025**
Dated:	**January 27, 2025**
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

Linda Morrison
Lisa Mitchell
Clare Parran
Sheldon Durrant
Randy Heimann
The MITRE Corporation

Common Criteria Testing Laboratory

Cody Cummins
Allison Keenan
Gossamer Security Solutions, Inc.
Columbia, 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 Nexus 9000 Series Switches Running NX-OS 10.4 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation 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 Columbia, MD, United States of America, and was completed in January 2025. 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.

The Target of Evaluation (TOE) is the Cisco Nexus 9000 Series Switches Running NX-OS 10.4.

The Target of Evaluation (TOE) identified in this VR 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 VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the (ETR) are consistent with the evidence provided.

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

The technical information included in this report was obtained from the *Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target*, version 0.9, January 21, 2025 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 Nexus 9000 Series Switches Running NX-OS 10.4 (Specific models identified in Section 8)
Protection Profile	*collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020
ST	*Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target*, version 0.9, January 21, 2025
Evaluation Technical Report	*Evaluation Technical Report for Cisco Nexus 9000 Series Switches Running NX-OS 10.4*, version 0.2, January 21, 2025
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	The MITRE Corporation

3 Architectural Information

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

The (TOE) is the Cisco Nexus 9000 Series Switches Running NX-OS 10.4 (herein after referred to as Cisco Nexus 9K Series, or the TOE).

The TOE is a purpose-built data center-class switch for use as an aggregation switch in the data center.

3.1 TOE Description

The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9200, 9300, 9400, 9500, and 9800. The software is comprised of the NX-OS software image Release 10.4.

The Cisco Nexus 9000 Series Switches 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. All security functionality is enforced on the Nexus 9000 Series switches.

NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself.

3.2 TOE Evaluated Platforms

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

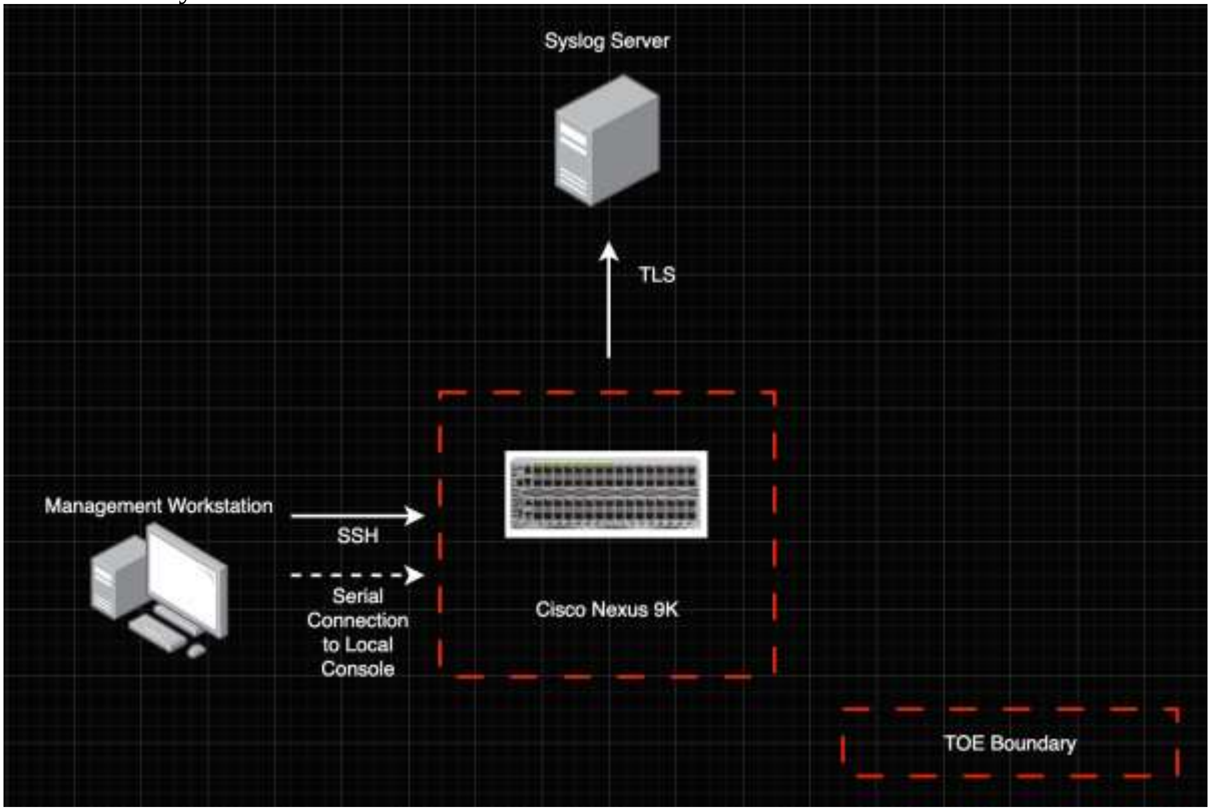
3.3 TOE Architecture

The TOE consists of one or more switches and includes the NX-OS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco NX-OS 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 internetworking device and forwarded to their configured destination.

If the TOE is to be remotely administered, then the management workstation must be connected to an internal network and SSHv2 must be used to securely connect to the TOE. Audit records are stored locally and are also remotely backed up to a remote syslog server. 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.

3.4 Physical Boundaries

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.



The figure above includes the following:

- The TOE model: Cisco Nexus 9000 Series Switches

The following are considered to be in the IT Environment:

- Management Workstation
- Syslog Server

For management purposes the TOE provides command line access to administer the TOE and remote access over SSH.

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 TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides circular audit trail. Audit logs are transmitted to an external audit server over a trusted channel protected with TLS.

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 authorized administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE is configured to transmit the audit messages to an external syslog server. Communication with the syslog server is protected by using TLS and the TOE can determine when communication with the syslog server fails. In the presence of a TLS communication failure, the TOE will continuously and automatically re-attempt to reestablish the syslog connection in case of a network disruption. In the case of a TLS protocol failure the administrator should review the configuration of both the TOE and the syslog server.

The audit logs can be viewed on the TOE using the appropriate NX-OS 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).

The NX-OS software calls the CiscoSSL FOM Cryptographic implementation version 7.3a and has been validated for conformance to the requirements of FIPS 140-2 Level 1.

The TOE provides cryptography in support of remote administrative management via SSHv2 and secure the session between the TOE and remote syslog server using TLS.

4.3 Identification and authentication

The TOE performs one type of authentication: authentication for the Authorized Administrator of the TOE using a local user database.

The TOE provides authentication services for administrative users wishing 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 is configured to require a minimum password length of 8 characters as well as password-strength checking that disables the use of weak passwords. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

After a configurable number of incorrect login attempts, Cisco Nexus 9K Series will lockout the account until an Authorized Administrator takes action.

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

4.4 Security management

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to configure thresholds for SSH rekeying;
- Ability to re-enable an Administrator account;
- Ability to set the time which is used for time-stamps;
- Ability to configure the reference identifier for the peer;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to import X.509v3 certificates to the TOE's trust store;
- Ability to manage the trusted public keys database;

The Cisco Nexus 9K Series switch supports the following predefined roles:

- network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the Nexus 9000 Series.
- network-operator - This role has read access to the entire NX-OS device.
- server-admin - Complete read access to the entire NX-OS device and upgrade capability.

All administrators are considered to be security administrators in this ST. The Cisco Nexus 9K Series has a CLI that can be administered either remotely using SSHv2 or locally via a console that is directly connected via a serial cable.

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 NX-OS is not a general-purpose operating system and access to Cisco NX-OS memory space is restricted to only Cisco NX-OS functions.

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. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE can verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

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 administrator can also terminate their own session by exiting out of the CLI.

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 for remote CLI access. Nexus 9K also allows a trusted channel to be established with a syslog server using TLS.

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

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

Clarification of scope

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.

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 collaborative 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.
- Apart from the Admin Guide, additional customer documentation for the specific network device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Cisco Nexus 9000 Series Switches Running NX-OS 10.4 Common Criteria Operational User Guidance and Preparative Procedures*, Version 0.9, January 21, 2025

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

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 proprietary Detailed Test Report for Cisco Nexus 9000 Series Switches Running NX-OS 10.4, Version 0.2, January 21, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (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 a Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration includes the following models, all running NX-OS 10.4:

Series	Models
Nexus 9200	N9K- C92348GC-X
Nexus 9300	N9K-C93108TC-FX, N9K-C9348GC-FXP, N9K-C93216TC-FX2, N9K-C93180YC-FX, N9K-C93240YC-FX2, N9K-C93360YC-FX2, N9K-C9364C, N9K-C9332C, N9K-C9336C-FX2, N9K-C9364C-GX, N9K-C9316D-GX, N9K-C93600CD-GX, N9K-C93400LD-H1
Nexus 9400	N9K-C9400-Sup-A
Nexus 9500	N9K-C9504, N9K-C9508, N9K-C9516, N9K-SUP-A+, N9K-SUP-B+, N9K-SC-A
Nexus 9800	N9K-C9804, N9K-C9808

8.2 Excluded Functionality

The functionality listed below will be disabled by configuration, as described in the Guidance documents (AGD). The excluded functionality does not affect conformance to the collaborative Protection Profile for Network Devices v2.2e.

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.
NTP	NTP will be disabled in the evaluated configuration.
DCNM GUI	The DCNM GUI was not included in the evaluated configuration.
Bash shell	Bash shell interface was not included in the evaluation.

PTP	PTP is not included in the evaluation.
HTTP Server	HTTP web server will be disabled in the evaluated configuration.
IPsec	IPsec is not included in the evaluated configuration.
LDAP	LDAP is not included in the evaluated configuration.
RADIUS	RADIUS is not included in the evaluation.
TACACS+	TACACS+ will be disabled in the evaluated configuration.

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 Nexus 9000 Series Switches Running NX-OS 10.4 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 Nexus 9000 Series Switches Running NX-OS 10.4 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

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

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

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

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

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. The public search for vulnerabilities did not uncover any residual vulnerability.

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

- 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),
- 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 January 7, 2025. The search was conducted with the following terms: “"Cisco Nexus 9000", "Cisco Nexus 9300", "Cisco Nexus", "Cisco", "Nexus", "NX-OS", "N9K", "Intel Xeon D-1633N", "Intel Xeon D-1526", "CiscoSSL", "Intel Xeon D-1528", "Intel Xeon D-1623N", "Intel Xeon D-1530", "Cisco Nexus 9400", "Cisco Nexus 9500", "Cisco Nexus 9800”.

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

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

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Cisco Nexus 9000 Series Switches Running NX-OS 10.4 Common Criteria Operational User Guidance and Preparative Procedures*, Version 0.9, January 21, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the NDcPP22e and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target, Version 0.9, January 21, 2025.*

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 VR:

[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.

[5] *Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target*, Version 0.9, January 21, 2025 (ST).

[6] *Assurance Activity Report for Cisco Nexus 9000 Series Switches Running NX-OS 10.4*, Version 0.2, January 21, 2025 (AAR).

[7] *Detailed Test Report for Ciso Nexus 9000 Series Switches Running NX-OS 10.4*, Version 0.2, January 21, 2025 (DTR).

[8] *Evaluation Technical Report for Cisco Nexus 9000 Series Switches Running NX-OS 10.4*, Version 0.2, January 21, 2025 (ETR).