

# **National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme**



## **Validation Report for the Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18**

**Report Number:** CCEVS-VR-VID11661-2026

**Dated:** April 9, 2026

**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**

Lori Sarem

Sheldon Durrant

Randy Heimann

Lisa Mitchell

Jaemon Reyes

Charles Schmidt

Jenn Dotson

### **The MITRE Corporation**

### **Common Criteria Testing Laboratory**

Kevin Steiner

Khushmit Kaur

Joon Sim

### **Lightship Security USA, Inc.**

## Table of Contents

|      |                                                                    |    |
|------|--------------------------------------------------------------------|----|
| 1.   | Executive Summary .....                                            | 1  |
| 2.   | Identification .....                                               | 2  |
| 3.   | Architectural Information .....                                    | 4  |
| 3.1. | TOE Description .....                                              | 4  |
| 3.2. | TOE Evaluated Configuration .....                                  | 4  |
| 3.3. | TOE Architecture.....                                              | 4  |
| 3.4. | Physical Boundary .....                                            | 4  |
| 4.   | Security Policy .....                                              | 6  |
| 4.1. | Security Audit .....                                               | 6  |
| 4.2. | Cryptographic Support.....                                         | 6  |
| 4.3. | Identification and Authentication .....                            | 6  |
| 4.4. | Security Management .....                                          | 7  |
| 4.5. | Packet Filtering .....                                             | 7  |
| 4.6. | Protection of the TSF .....                                        | 8  |
| 4.7. | TOE Access .....                                                   | 8  |
| 4.8. | Trusted Path/Channels .....                                        | 9  |
| 5.   | Assumptions and Clarification of Scope.....                        | 10 |
| 6.   | Documentation .....                                                | 11 |
| 7.   | IT Product Testing .....                                           | 12 |
| 7.1. | Developer Testing .....                                            | 12 |
| 7.2. | Evaluation Team Independent Testing .....                          | 12 |
| 8.   | TOE Evaluated Configuration .....                                  | 13 |
| 8.1. | Evaluated Configuration .....                                      | 13 |
| 8.2. | Excluded Functionality .....                                       | 13 |
| 9.   | Results of the Evaluation .....                                    | 14 |
| 9.1. | Evaluation of Security Target (ASE).....                           | 14 |
| 9.2. | Evaluation of Development Documentation (ADV) .....                | 14 |
| 9.3. | Evaluation of Guidance Documents (AGD) .....                       | 14 |
| 9.4. | Evaluation of Life Cycle Support Activities (ALC) .....            | 15 |
| 9.5. | Evaluation of Test Documentation and the Test Activity (ATE) ..... | 15 |
| 9.6. | Vulnerability Assessment Activity (VAN).....                       | 15 |

9.7. Summary of Evaluation Results..... 16

10. Validator Comments ..... 18

11. Annexes..... 19

12. Security Target..... 20

13. Glossary ..... 21

14. Acronym List ..... 22

15. Bibliography ..... 23

List of Tables

Table 1: Evaluation Identifiers..... 2

## **1. Executive Summary**

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 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 (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in April 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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 3.0e, PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, PP-Module for MACsec Ethernet Encryption, Version 1.0, and Functional Package for Secure Shell (SSH), Version 1.0.

The TOE is Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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 (CCEVS) 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 Security Target 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 TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The 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                                                             |
| Evaluated Product     | Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18                                                 |
| Sponsor and Developer | Cisco Systems, Inc<br>170 West Tasman Drive, San Jose, CA 95134                                                                 |
| CCTL                  | Lightship Security USA, Inc.<br>3600 O'Donnell St., Suite 2<br>Baltimore, MD 21224                                              |
| CC Version            | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.                            |
| CEM                   | Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017. |

| Item                        | Identifier                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protection Profile          | collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E)<br>PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_V1.3)<br>PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACSEC_V1.0)<br>Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0) |
| ST                          | Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Security Target, v1.1, April 6, 2026                                                                                                                                                                                                        |
| Evaluation Technical Report | Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Evaluation Technical Report, v1.3, April 2026                                                                                                                                                                                               |
| Conformance Result          | CC Part 2 extended, CC Part 3 conformant                                                                                                                                                                                                                                                                                    |
| Evaluation Personnel        | Kevin Steiner, Khushmit Kaur, Joon Sim                                                                                                                                                                                                                                                                                      |
| CCEVS Validators            | The MITRE Corporation: Lori Sarem, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Jaemond Reyes, Charles Schmidt, Jenn Dotson                                                                                                                                                                                               |

### **3. Architectural Information**

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

#### **3.1. TOE Description**

The Cisco 8200, 8300, 8400, 8500 Series Secure Routers (herein after referred to as the C8000 respectively) are purpose-built, routing platforms that include VPN functionality and MACsec encryption provided by the TOE hardware and the Cisco IOS-XE software. The TOE includes the hardware models as defined in Table 2.

The TOE is a Network Device that includes VPN functionality and MACsec encryption as defined in CPP\_ND\_V3.0E, PKG\_SSH\_V1.0, MOD\_VPNGW v1.3, and MOD\_MACSEC\_V1.0. The TOE is comprised of hardware, software and firmware. The hardware is comprised of the C8000 routers as described in 3.4 Physical Boundary. The software is comprised of the Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.18. The firmware is comprised of the IOS Common Cryptographic Module (IC2M) and the Marvell 88x7121M.

#### **3.2. TOE Evaluated Configuration**

Detail regarding the evaluated configurations and any excluded functionality is provided in Section 8.

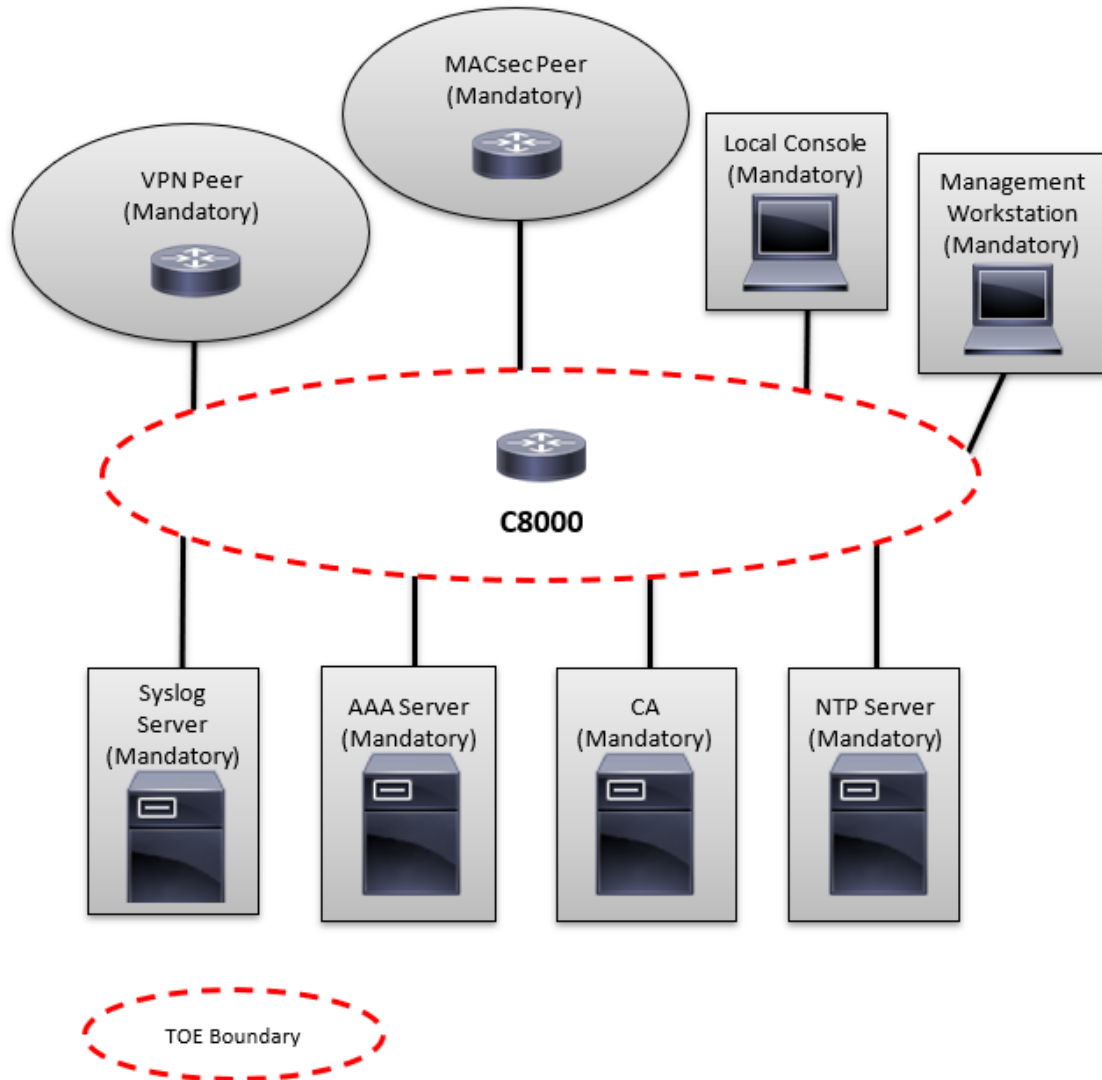
#### **3.3. TOE Architecture**

The TOE consists of one physical device and includes Cisco IOS-XE version 17.18 software. Consult the ST for detailed information about available hardware and module configurations. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.18. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router 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.

The network on which they reside is considered part of the operational environment. The following components are also considered to be part of the operational environment: VPN Peer, MACsec Peer, Management Workstation, Radius AAA (Authentication) Server, Audit (Syslog) Server, Local Console, Certificate Authority (CA), and NTP Server(s).

#### **3.4. Physical Boundary**

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



**Figure 1 TOE boundary**

## 4. Security Policy

This section summarizes the security functionality of the TOE:

### 4.1. Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. 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 the administrator with a circular audit trail stored in persistent memory, with a configurable maximum size. When the log reaches the configured threshold, the TOE overwrites the oldest records. Audit logs are backed up over an encrypted channel to an external audit server.

### 4.2. Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates for all processors listed in **Error! Reference source not found.**4 of the ST. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5b. These cryptographic modules are implemented as firmware, and the cryptographic operational environment for each of these modules is:

- Intel Xeon D-1736NT (Ice Lake), Marvell Octeon 10 - MV-CN10208-C160, Marvell Octeon 10 - MV-CN10612-C190, Marvell Octeon 10 - MV-CN10616-C250, Marvell Octeon 10 - MV-CN10616-C250, Marvell Octeon 10 - MV-CN10624-C250 for the IOS Common Cryptographic Module (IC2M) Rel5a (A1462)

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers. Additional information on cryptographic services provided by the TOE are described in **Error! Reference source not found.**5 of the ST.

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

### 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 TOE

supports use of IKEv2 pre-shared keys for authentication of IPsec tunnels. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. 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. The TOE supports the 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 provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding 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 ability to securely manage:

- Administration of the TOE locally and remotely;
- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- NTP configurations;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality.

Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authorized administrators.

Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

#### **4.5. Packet Filtering**

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers. More accurately, these tunnels are sets of

security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

The TOE is also capable of rejecting any MACsec PDUs in a given session that contain a SCI that is different from the one that is used to establish that session. The SCI is derived from the MACsec peer's MAC address and port to uniquely identify the originator of the MACsec PDU. Only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), MAC control frames EtherType 0x876F are permitted in the MACsec communication between peers and others are discarded.

#### **4.6. 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 also able to detect replay of information received via secure channels (MACsec). The detection applies to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE has an internal clock; however, the TOE synchronizes time with an NTP server and then internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

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

#### **4.7. 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. Sessions can also be terminated if an Authorized Administrator enters the "exit" or "logout" command.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

#### **4.8. Trusted Path/Channels**

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 which has the ability to be encrypted further using IPsec and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect communications with a CA. In addition, IPsec is used to secure communications between the TOE and external entities, including remote authentication servers and NTP servers (via NTPv4 over IPsec).

## 5. Assumptions and 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 3.0e (NDcPP30e)
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0 (MOD\_MACSEC\_V1.0)
- *PP-Module for VPN Gateways*, Version 1.3, (VPNGW13)
- *Functional Package for Secure Shell (SSH)*, Version 1.0 (PKG\_SSH\_V1.0)

That information has not been reproduced here and the NDcPP30e/ MOD\_MACSEC\_V1.0/VPNGW13/ PKG\_SSH\_V1.0 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 CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0 as described for this TOE in the ST. 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 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 in accordance with the evaluation activities specified in CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0 and performed by the evaluation team.
- This evaluation covers only the specific software version 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 TOE models was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device in the evaluated configuration.
- 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 CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

## **6. Documentation**

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures, v1.1, April 6, 2026*
- *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Flaw Remediation and Reporting Procedures, v0.3, February 26, 2026*
- *Flaw Remediation and Reporting Procedures, v0.3, February 26, 2026*

Any additional customer documentation provided with the product or that is available online was not included in the scope of the evaluation and 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 evaluation team. It is derived from information contained in Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Assurance Activity Report, v1.4, April 2026 provides an overview of testing and the prescribed evaluation activities.

### **7.1. Developer Testing**

No evidence of developer testing is required in the SARs or Evaluation Activities.

### **7.2. Evaluation Team Independent Testing**

The evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from October 2025 until April 2026. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e/ MOD\_MACSEC\_V1.0/ VPNGW13/ PKG\_SSH\_V1.0 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. TOE Evaluated Configuration

This section briefly identifies the evaluated configuration(s) and any excluded and out of scope functionality.

### 8.1. Evaluated Configuration

The TOE consists of the following models.

Cat8200 hardware models included in this evaluation:

- C8235-E-G2
- C8231-E-G2
- C-NIM-4X
- C-NIM-8T
- C-NIM-8M
- C-NIM-WAN-2X
- C-NIM-WAN-4S

Cat8300 hardware models included in this evaluation:

- C8355-G2
- C8375-E-G2
- C-NIM-4X
- C-NIM-8T
- C-NIM-8M
- C-NIM-WAN-2X
- C-NIM-WAN-4S

Cat8400 hardware models included in this evaluation:

- C8455-G2
- C8475-G2

Cat8500 hardware models included in this evaluation:

- C8550-G2
- C8570-G2

### 8.2. Excluded Functionality

The following functionality is excluded from the evaluation.

| Excluded Functionality                  | Exclusion Rationale                                                                                                     |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Non-FIPS 140-2 mode of operation        | This mode of operation includes non-FIPS allowed operations.                                                            |
| USB ports                               | USB ports are not used for TOE functionality                                                                            |
| FTP (File Transfer Protocol)            | FTP is not used in the evaluated configuration. Secure file transfer is performed using trusted channels (e.g., IPsec). |
| Telnet                                  | Telnet is not used in the evaluated configuration because it does not provide secure communication.                     |
| SNMP                                    | SNMP server functionality is not used in the evaluated configuration.                                                   |
| SSH Client                              | SSH client functionality is not included in the evaluation, as FCS_SSHC_EXT.1 is not claimed.                           |
| SSH keyboard-interactive authentication | Keyboard-interactive authentication is not allowed 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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0.

### **9.1. Evaluation of 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 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 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 Development Documentation (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 ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities 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 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 Life Cycle Support Activities (ALC)**

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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 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 Test Evaluation Activities 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 Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Vulnerability Assessment, v1.3, March 2026, report prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on March 27, 2026, did not uncover any residual vulnerability.

The evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): <https://web.nvd.nist.gov/view/vuln/search>
- Common Vulnerabilities and Exposures: [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)
- CVE Details: <https://www.cvedetails.com/vulnerability-search.php>
- CISA - Known Exploited Vulnerabilities Catalog: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Cisco security advisories (<https://www.cisco.com/security/>)

The evaluation team performed a search using the following keywords:

- Cisco 8200

- Cisco 8300
- Cisco 8400
- Cisco 8500
- C8235-E-G2
- C8231-E-G2
- C8355-G2
- C8375-E-G2
- C8455-G2
- C8475-G2
- C8550-G2
- C8570-G2
- Marvell Octeon 10
- Marvell Octeon 10 - MV-CN10208-C160
- Marvell Octeon 10 - MV-CN10612-C190
- Marvell Octeon 10 - MV-CN10616-C250
- Marvell Octeon 10 - MV-CN10624-C250
- Intel Xeon D-1736NT (Ice Lake)
- Intel Xeon D-1736NT firmware
- Marvell 88x7121M
- Marvell 88EC808
- Synopsys VCS version R-2020.12-SP2-0\_Full64
- Mentor Questa Sim 10.7
- Comira MV88EC808
- Cisco IOS-XE 17.18
- IC2M Rel5a
- IC2M Rel5b
- CiscoSSL
- CiscoSSH

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 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 followed the procedures defined in the CEM and performed the Evaluation Activities in CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0, and correctly verified that the product meets the claims in the ST.

## **10. Validator Comments**

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this VR. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated was scoped exclusively to the hardware platforms and network modules identified and the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the TOE in the operational environment need to be assessed separately and no further conclusions can be drawn about their 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 CPP\_ND\_V3.0E, MOD\_VPNGW\_V1.3, MOD\_MACSEC\_V1.0, and PKG\_SSH\_V1.0 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**

*Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18*

*Security Target, v1.1, April 6, 2026 Security Target, v1.1, April 6, 2026*

## 13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

## 14. Acronym List

|       |                                                          |
|-------|----------------------------------------------------------|
| CAVP  | Cryptographic Algorithm Validation Program (CAVP)        |
| CCEVS | Common Criteria Evaluation and Validation Scheme         |
| CCIMB | Common Criteria Interpretations Management Board         |
| CCTL  | Common Criteria Testing Laboratories                     |
| CEM   | Common Evaluation Methodology for IT Security Evaluation |
| LS    | Lightship Security USA CCTL                              |
| DHCP  | Dynamic Host Configuration Protocol                      |
| ETR   | Evaluation Technical Report                              |
| IT    | Information Technology                                   |
| LDAP  | Lightweight Directory Access Protocol                    |
| MFD   | Multi-Function Device                                    |
| NIAP  | National Information Assurance Partnership               |
| NIST  | National Institute of Standards and Technology           |
| NSA   | National Security Agency                                 |
| NVLAP | National Voluntary Laboratory Assessment Program         |
| OS    | Operating System                                         |
| OSP   | Organizational Security Policies                         |
| PCL   | Products Compliant List                                  |
| ST    | Security Target                                          |
| TOE   | Target of Evaluation                                     |
| VR    | Validation Report                                        |

## 15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices, Version 3.0e*  
(CPP\_ND\_V3.0E)
6. *PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3*  
(MOD\_VPNGW\_V1.3)
7. *PP-Module for MACsec Ethernet Encryption, Version 1.0*  
(MOD\_MACSEC\_V1.0)
8. *Functional Package for Secure Shell (SSH), Version 1.0* (PKG\_SSH\_V1.0)
9. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Security Target*, v1.1, April 6, 2026
10. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures*, v1.1, April 6, 2026
11. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Flaw Remediation and Reporting Procedures*, v0.3, February 26, 2026
12. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Assurance Activity Report*, v1.4, April 2026
13. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Vulnerability Assessment*, v1.3, March 2026
14. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Evaluation Technical Report*, v1.3, April 2026
15. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 Detailed Test Report*, v1.3, April 2026
16. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8475-G2 NDcPP v3.0e Test Evidence*, v1.2, March 2026
17. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8475-G2 VPNGW v1.3 Test Evidence*, v1.1, February 2026
18. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8475-G2 SSH v1.0 Test Evidence*, v1.3, April 2026
19. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8475-G2 MACsec v1.0 Test Evidence*, v1.2, March 2026

20. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8570-G2 NDcPP v3.0e Test Evidence, v1.2, March 2026*
21. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8570-G2 VPNGW v1.3 Test Evidence, v1.1, February 2026*
22. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8570-G2 SSH v1.0 Test Evidence, v1.3, April 2026*
23. *Cisco 8200, 8300, 8400, 8500 Series Secure Routers (C8000) running IOS-XE 17.18 C8570-G2 MACsec v1.0 Test Evidence, v1.2, March 2026*