Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6

20 March 2023

560-LSS

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 (hereafter referred to as the Target of Evaluation, or TOE), from **Cisco Systems, Inc.** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **20 March 2023** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6
Developer	Cisco Systems, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

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

U.S. Government Approved Protection Profile - Extended Package for Wireless LAN Access Systems Version 1.0, May 29 2015

1.2 TOE DESCRIPTION

The TOE is a distributed Wireless Local Area Network (WLAN) access system consisting of a Wireless LAN Controller (WLC) and one or more Access Points (AP). A WLAN Access System ensures wireless clients are authenticated by a centralized authentication server and provides an encrypted IEEE 802.11 link to protect wireless communications from unauthorized disclosure and/or modification. A WLAN Access System also provides for central management and administration of the wireless infrastructure within an organization.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

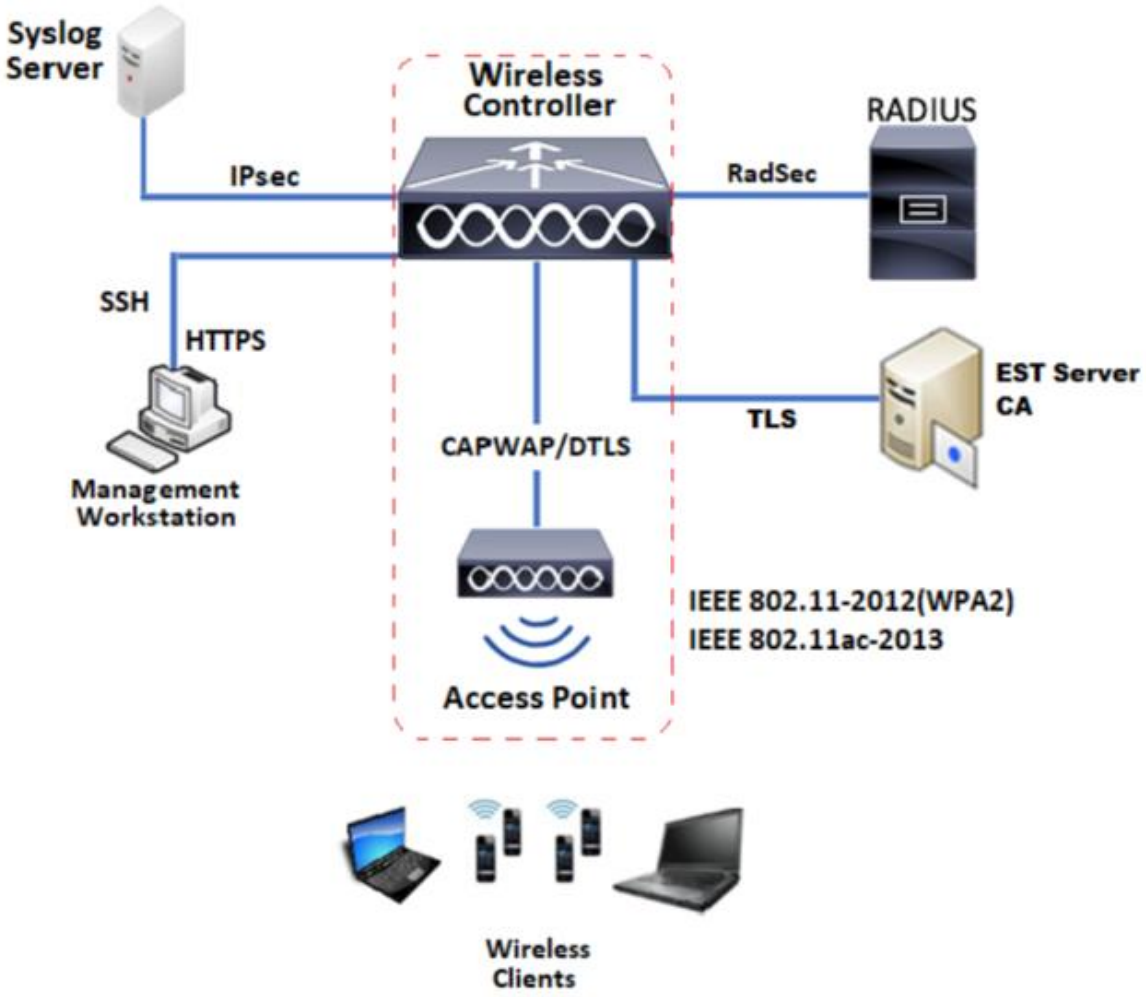

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

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

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Module	Certificate Number
CiscoSSL FOM 7.0a	A877
CiscoSSL FOM 7.0b	A2452
IOS Common Cryptographic Module Rel5a	A1462
Cisco Aironet 3800 88W8964C	AES 4114
Qualcomm Lithium AES engine-256w v1.1	AES 5663
Broadcom Crypto Hardware Module aes_core_gcm.vhd(bca) rev 1.1	C1273
Broadcom Crypto Hardware Module aes_core_gcm.vhd(bca) rev 1.2	C1275

The following wireless implementations are used by the TOE and have been certified by the Wi-Fi Alliance:

Table 3: Wi-Fi Alliance Certificates

Wireless Module	Certificate Number
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9130AX AP	WFA98109
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9120AX AP	WFA98120

Wireless Module	Certificate Number
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9115AX AP	WFA98113
Cisco Catalyst 9800-80 Wireless Controller and Cisco C9105AX AP	WFA100774
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 1560 Series AP	WFA97683
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 4800 Series AP	WFA97651
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 3800 Series AP	WFA97641
Cisco Catalyst 9800-80 Wireless Controller and Cisco Aironet 2800 Series AP	WFA97646
Cisco Catalyst 9800-80 Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98227
Cisco Catalyst 9800-80 Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98232
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9130AX AP	WFA98108
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9120AX AP	WFA98119
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9115AX AP	WFA98112
Cisco Catalyst 9800-40 Wireless Controller and Cisco C9105AX AP	WFA100773
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 1560 Series AP	WFA97655
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 4800 Series AP	WFA97650
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 3800 Series AP	WFA97640
Cisco Catalyst 9800-40 Wireless Controller and Cisco Aironet 2800 Series AP	WFA97645
Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98226
Cisco Catalyst 9800-40 Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98231
Cisco Catalyst 9800-L Wireless Controller and Cisco C9130AX AP	WFA97958
Cisco Catalyst 9800-L Wireless Controller and Cisco C9120AX AP	WFA98117
Cisco Catalyst 9800-L Wireless Controller and Cisco C9115AX AP	WFA97959
Cisco Catalyst 9800-L Wireless Controller and Cisco C9105AX AP	WFA100294
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 1560 Series AP	WFA97654
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 4800 Series AP	WFA97649
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 3800 Series AP	WFA97429
Cisco Catalyst 9800-L Wireless Controller and Cisco Aironet 2800 Series AP	WFA97644
Cisco Catalyst 9800-L Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98225
Cisco Catalyst 9800-L Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98230
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9130AX AP	WFA98110
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9120AX AP	WFA98121
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9115AX AP	WFA98114
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco C9105AX AP	WFA100775

Wireless Module	Certificate Number
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 1560 Series AP	WFA97684
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 4800 Series AP	WFA97652
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 3800 Series AP	WFA97642
Cisco Catalyst 9800 Cloud Wireless Controller and Cisco Aironet 2800 Series AP	WFA97647
Cisco Catalyst 9800-CL Wireless Controller and Cisco Catalyst Industrial Wireless 6300 Series AP	WFA98228
Cisco Catalyst 9800-CL Wireless Controller and Cisco 6300 Series Embedded Services AP	WFA98233

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).

  If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
- For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
- The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
- The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.2 CLARIFICATION OF SCOPE

The functionality listed below is not included in the evaluated configuration.

- Operating in non-FIPS 140-2 and non-CC mode
- WPA and WPA2 with TKIP encryption
- Cisco Catalyst 9800-CL for public cloud
- Cisco CleanAir

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profile.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	Cisco Catalyst 9800 Series Wireless Controllers 17.6.01 • C9800-L-universalk9_wlc.17.6.01.SPA.bin • C9800-40-universalk9_wlc.17.6.01.SPA.bin • C9800-80-universalk9_wlc.17.6.01.SPA.bin • C9800-CL-universalk9.17.6.01.ova Note: The Access Points software images v17.6.01 are embedded in each WLC v17.06.01 image and are not separately downloaded and installed.
TOE Hardware	Wireless Controllers (WLC): • Cisco Catalyst 9800-80 (C9800-80-K9) • Cisco Catalyst 9800-40 (C9800-40-K9) • Cisco Catalyst 9800-L (C9800-L-F-K9, C9800-L-C-K9) Access Points (AP): • Cisco Catalyst 9130 Series Wi-Fi 6 Access Points (C9130AXI-x, C9130AXE-x, C9130AXE-STA-x) • Cisco Catalyst 9120 Series Wi-Fi 6 Access Points (C9120AXI-x, C9120AXE-x, C9120AXP-x) • Cisco Catalyst 9115 Series Wi-Fi 6 Access Points (C9115AXI-x, C9115AXE-x) • Cisco Catalyst 9105 Series Wi-Fi 6 Access Points (C9105AXI-x, C9105AXW-x, C9105AXIT-x, C9105AXWT-x) • Cisco Catalyst IW6300 Series Access Points (IW-6300H-AC-X-K9, IW-6300H-DC-X–K9, IW-6300H-DCW-X–K9) • Cisco ESW6300 Access Point (ESW-6300-CON-X-K9) • Cisco Aironet 1562 Series Access Points (AIR-AP1562I-x-K9, AIR-AP1562E-x-K9, AIR-AP1562D-x-K9) • Cisco Aironet 4800 Access Point (AIR-AP4800-x-K9, AIR-AP4800-x-K9C) • Cisco Aironet 3800 Series Access Points (AIR-AP3802I-x-K9, AIR-AP3802I-x-K9C, AIR-AP3802e-x-K9, AIR-AP3802E-x-K9C, AIR-AP3802p-x-K9, AIR-AP3802p-x-K9C) • Cisco Aironet 2800 Series Access Points (AIR-AP2802I-x-K9, AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9, AIR-AP2802E-x-K9C)

TOE Virtual	Wireless Controllers (WLC): • Cisco Catalyst 9800-CL (C9800-CL-K9) on VMware ESXi 6.7 running on Cisco Rack Servers UCSC-C220-M5, UCSC-C240-M5, or UCSC-C480-M5
Environmental Support	• EST Server • Certificate Authority • RADIUS Authentication Server (FreeRADIUS 3.0.x or higher) • Syslog Server • Management Workstation (with a TLS web browser or SSH client)

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6, CC Configuration Guide, v0.8 February 10, 2023

The following documents are available for download to assist in the configuration and installation of the TOE:

a) Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide
b) Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide
c) Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide
d) Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide
e) Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide
f) Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
g) Cisco Catalyst 9800 Wireless Controller Series Deployment Guide
h) Cisco Catalyst 9800 Wireless Controller Series Web UI Deployment Guide
i) Understanding Catalyst 9800 Wireless Controllers Configuration Mode
j) Understand FlexConnect on Catalyst 9800 Wireless Controller
k) C9800 Radio Resource Management Deployment Guide
l) Security Configuration Guide, Cisco IOS XE Gibraltar 17.4.x
m) Cisco Catalyst 9800 Series Wireless Controller Command Reference, Cisco IOS XE Bengaluru 17.6.x
n) Cisco Catalyst 9130AX Series Access Point Getting Started Guide
o) Cisco Catalyst 9120AX Series Access Point Getting Started Guide
p) Cisco Catalyst 9115AX Series Access Point Getting Started Guide
q) Cisco Catalyst 9105AX Series Access Point Getting Started Guide
r) Cisco Catalyst IW6300 Heavy Duty Series Access Point Hardware Installation Guide
s) Cisco ESW6300 Embedded Services Access Point
t) Cisco Aironet 1560 Series Outdoor Access Point Hardware Installation Guide
u) Getting Started Guide - Cisco Aironet 2800 Series Access Points

v) Getting Started Guide - Cisco Aironet 3800 Series Access Points
w) Cisco Aironet Series 2800/3800 Access Point Deployment Guide
x) Cisco Aironet 4800 Series Access Points Getting Started Guide
y) Cisco Aironet Series 4800 Access Point Deployment Guide
z) Cisco Catalyst 9130 Series Access Point Deployment Guide
aa) Security for VPNs with IPsec Configuration Guide, Cisco IOS XE 17
bb) Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.6.x

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations were present in the TOE.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **19 October 2022** and included the following search terms:

Cisco Catalyst 9800-40 Wireless Controller	Cisco ESW6300 Access Point	ACT2lite (Anti-Counterfeit Technology 2 Lite) 15-14497-02
Cisco Catalyst 9800-CL Wireless Controller for Private Cloud (vSphere)	Cisco Aironet 1562 Series Access Points	Microsemi SmartFusion2 SoC FPGA M2S010TS
Cisco Catalyst 9800-80 Wireless Controller	Cisco Aironet 4800 Access Point	Cisco IOS-XE 17.6.01
Cisco Catalyst 9800-L Wireless Controller	Cisco Aironet 3800 Series Access Points	OpenResty 1.15.8.3
Cisco UCSC-C220-M5	Cisco Aironet 2800 Series Access Points	CiscoSSL 7.1.3
Cisco UCSC-C240-M5	Intel Xeon Silver 4116T	IC2M Rel5a
Cisco UCSC-C480-M5	Intel Xeon Broadwell D-1548	CiscoSSH 1.7.22
Cisco Catalyst 9130 Series Wi-Fi 6 Access Points	Intel Xeon Broadwell D-1563N	Lightweight AP software 17.6.01
Cisco Catalyst 9120 Series Wi-Fi 6 Access Points	Intel Xeon Platinum 8160M	CiscoSSL 7.1.220
Cisco Catalyst 9115 Series Wi-Fi 6 Access Points	Qualcomm IPQ8078 ARMv8	dnsmasq 2.83-1

Cisco Catalyst 9105 Series Wi-Fi 6 Access Points	Broadcom BCM49408 ARMv8	U-Boot
Cisco Catalyst 9105 Series Wi-Fi 6 Access Points	Broadcom BCM47622 ARMv7	
Cisco Catalyst IW6300 Series Access Points	Marvell Armada 390 88F6920 ARMv7	

Vulnerability searches were conducted using the following sources:

Vendor security advisories https://tools.cisco.com/security/center/softwarechecker.x	US-CERT https://www.kb.cert.org/vuls/html/search
NIST National Vulnerabilities Database (NVD) https://web.nvd.nist.gov/view/vuln/search	CISA - Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Common Vulnerabilities and Exposures https://cve.mitre.org/cve/	OpenSSL Vulnerabilities https://www.openssl.org/news/vulnerabilities.html

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 Security Target, version 1.7, March 17, 2023
Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 Evaluation Technical Report, version 1.2, March 20, 2023
Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.6 Assurance Activity Report, version 1.2, March 20, 2023