Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Cisco WLAN 8.0

Certification Report
2016/100

07-10-2016
Version 1.0

Amendment Record

Version	Date	Description
1.0	07-10-2016	External

Executive Summary

This report describes the findings of the IT security evaluation of Cisco WLAN 8.0 against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Cisco WLAN 8.0. The TOE is a Wireless LAN (WLAN) Access System comprised of multiple products operating together to provide secure wireless access to wired and wireless networks end-to-end wireless encryption, and centralised administration of all WLAN controllers and Access Points (APs) in the system.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit** – auditable events are stored internally in the TOE. The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco WLAN generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity.
- **Cryptological Support** – The TOE provides cryptography in support of:
    - IPsec to secure communications between the WLC and RADIUS server
    - TLS/HTTPS for secure remote administration using WebGUI
    - TLS to secure communications between WLC remote syslog server
    - Data TLS to secure communications between APs and WLC
    - WPA2 to secure communications between APs and wireless clients.

  This cryptography in Wireless LAN Controller (WLC) and AP components has been validated for conformance to the requirements of FIPS 140-2 Level 2. The CMVP certificates are listed in the ST.
- **User Data -** The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE, and when packets must be padded, they are padded with zeros.
- **Identification and Authentication –** The TOE provides authentication services for administrative users of the TOE who connect locally to the Command Line Interface (CLI) via serial console of the WLAN Controller or remotely to the GUI over TLS. The TOE requires administrators to authenticate prior to being granted access to any of the management functionality

  Security Management – Through CLI and GUI of the Controller, the TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE.
  Protection of the TSF and resource allocation – The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorised Administrators. The TOE prevents reading of plaintext cryptographic keys and passwords.

- **TOE Access –** Administrative sessions can be set to terminate after a configurable idle-time limit. Once a session has been terminated the TOE requires administrators to re-authenticate to establish a new session. A customizable login-banner can be displayed at the CLI and GUI login prompts prior to allowing any administrative access to the TOE. Wireless client session establishment can be restricted by day, time, and ‘location’, which can be an IP address or WLAN ID.
- **Trusted Path / Channels –** The wireless connections between the APs and wireless clients are secured using Wi-Fi Protected Access 2 (WPA2).

The report concludes that the product has complied with the U.S Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems (WLANPP) Version 1.0, December 1, 2011 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC Australia and was completed on 12 August 2016. The status of the evaluation was concurrent for a large portion of the evaluation time.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor’s product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
d) Avoid the use of self signed certificates
e) Use the Command line interface local console instead of the web GUI.
f) Note that workstations used for remote administration of the TOE must be dedicated for performing administrative tasks on the TOE, and prevented from communicating (sending and receiving traffic) with assets not related to administration of the TOE
g) Note that Internet Explorer is not compatible with the WLC WebGUI.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification results of the IT security evaluation of the Cisco WLAN 8.0 against the requirements of the Common Criteria (CC) and the WLANPP

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is the Cisco WLAN 8.0.

Table 1 Identification Information

Description	**Version**
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco WLAN 8.0
Software Version	8.0.132.0
Hardware Platforms	Cisco 2504, 5508, 7510, 8510, and WiSM2 Controllers; Cisco 1142, 1262, 1530, 1552, 1570 series, 1600 series, 1700 series, 2600 series, 2700 series, 3502, 3600 series with 3000M add-on module, and 3700 series APs, and ISR 891 integrated AP.
Security Target	Cisco WLAN 8.0 Common Criteria Security Target Version 1.0, September 2016

Evaluation Technical Report	Cisco WLAN 8.0, Evaluation Technical Report, (T0080) REFERENCE: CSC-EFC-T0080-ETR EVALUATION-IN-CONFIDENCE, Version 1.0
Criteria	Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012
Methodology	Common Methodology for Information Technology Security version 3.1, Revision 4, September 2012
Conformance	U.S Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems (WLANPP) Version 1.0, December 1, 2011
Developer	Cisco Systems Inc. 170 West Tasman Drive, San Jose, California 95134 United States
Evaluation Facility	CSC Australia Pty Limited 12 Brindabella Circuit Brindabella Business Park ACT 2609 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is Cisco WLAN 8.0. The TOE is a Wireless LAN (WLAN) Access System comprised of multiple products operating together to provide secure wireless access to wired and wireless networks end-to-end wireless encryption, and centralised administration of all WLAN controllers and APs in the system.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit** – auditable events are stored internally in the TOE. The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco WLAN generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity
- **Cryptological Support** – The TOE provides cryptography in support of:
  - IPsec to secure communications between the WLC and RADIUS server
  - TLS/HTTPS for secure remote administration using WebGUI
  - TLS to secure communications between WLC remote syslog server
  - Data TLS to secure communications between APs and WLC
  - WPA2 to secure communications between APs and wireless clients.

  This cryptography in WLC and AP TOE components has been validated for conformance to the requirements of FIPS 140-2 Level 2. The CVMP certificates are listed in the ST.
- **User Data -** The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE, and when packets must be padded, they are padded with zeros.
- **Identification and Authentication** – The TOE provides authentication services for administrative users of the TOE who connect locally to the CLI via serial console of the WLAN Controller or remotely to the GUI over TLS. The TOE requires 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 and to enforce mandatory password complexity rules. All of the local and remote CLI and GUI connections the TOE support

password-based authentication of administrators against either a local user database or remote RADIUS server. For authentication of wireless clients a RADIUS server must be used (AAA servers are outside the TOE boundary). The TOE requires the wireless client to perform 802.1X authentication, relying on an authentication server to authenticate the client, before providing network access. The TOE acts as a pass through device between the wireless client and authentication server. The TOE facilitates authentication of wireless clients by performing the role of authenticator in an 802.1X authentication exchange. During an 802.1X authentication exchange, wireless client authentication is relayed by the WLC to a RADIUS server. The TOE will block access to the port until the authentication server returns an authentication success message and 802.11 temporal keys are derived and installed on the wireless client and AP. The TOE provides IPsec to protect the transfer of the Pairwise Master Key the WLC receives from the RADIUS server.

- **Security Management –** Through CLI, and GUI of the Controller, the TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Functions available to authorised administrators include, but are not limited to:
    - Enabling, disabling, and configuring audit collection
    - Modifying the behaviour of cryptographic functions
    - Configuring security of communications to/from an external servers including RADIUS and syslog servers
    - Adding/removing/modifying administrative accounts including specifying a maximum number of successive failed authentication attempts that will be permitted by remote administrators
    - Defining inactivity timeout limits for interactive interfaces to terminate inactive sessions
    - Creating custom login banners for interactive interfaces to be displayed at time of login.

  Accounts with access to CLI and GUI can have read-write access, or can be assigned to lesser sets of privileges that can be custom-defined. Authorised administrators are users who have successfully authenticated to the TOE, and have been granted the necessary privilege to perform some administrative actions, which may be limited to read-only actions.
- **Protection of the TSF and resource allocation –** The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorised administrators. The TOE prevents reading of plaintext cryptographic keys and passwords. Additionally none of the components of the TOE includes a general-purpose operating systems and access to the memory space is restricted to only system functions. Authorised administrators have the option to verify the integrity of software updates using cryptographic signatures prior to the software updates being installed. Self-testing is performed during boot-up to verify correct operation of system hardware and the cryptographic module. When power-on self-tests (POST) fail for any controller or AP, the device will not progress to an operational mode (e.g. will not forward network traffic, nor authenticate wireless clients or administrators, etc.).

System resources used to support administrative interfaces are protected by allowing authorised administrators to limit the number of concurrent sessions. TOE components will detect and drop (not forward) replayed packets received at network interfaces (including wireless radio interfaces).

Each TOE component internally maintains the date and time, and clocks are synchronized among components. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, and/or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source.

- **TOE Access –** Administrative sessions can be set to terminate after a configurable idle-time limit. Once a session has been terminated the TOE requires administrators to re-authenticate to establish a new session. A customizable login-banner can be displayed at the CLI and GUI login prompts prior to allowing any administrative access to the TOE. Wireless client session establishment can be restricted by day, time, and location, which can be an IP address or WLAN ID.
- **Trusted Path / Channels –** The wireless connections between the APs and wireless clients are secured using Wi-Fi Protected Access 2 (WPA2). Specifically, the TOE uses Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP), as defined in the WPA2 standard. TSF data (command and control data, audit data, etc.) transmitted among controllers and APs of the TOE are secured with Data TLS (for CAPWAP over DTLS) using ciphersuites required by the WLANPP for the TLS connections.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- Wireless controllers
- Wireless integrated service module (WiSM2) controllers
- Access Points and antennae.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Cisco WLAN Common Criteria Operational User Guidance and Preparative Procedures (Ref 2).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from WLANPP (Ref 3) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 4) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

The following components are outside of the scope of the TOE:

- The wireless connections between the APs and wireless
- Management workstation
- AAA server
- Syslog server
- Certification authority
- File server and
- NTP server
- RADIUS sever

2.6 Usage

2.6.1 Evaluated Configuration

The TOE consists of the Cisco WLAN v8.0.132.0 software. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Cisco WLAN 8.0 Controller Configuration Guide (Ref 6).

2.6.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- Shipment of units from Cisco Distributors to the user is via a commercial courier company who will pick up the unit from the Distribution Site and deliver it directly to the user.
- For hardware components; using the packing slip and information on the stickers, the customer must check that the product number and serial numbers on the received hardware match what was ordered. Any discrepancies must be immediately reported to Cisco using the contact information on the packing slip.
- For Software, the customer will access CCO (Cisco Connection Online) to download images. Customers will be prompted for their login and password. To create an account on CCO a user must have a valid support contract with Cisco and access to the contract number. Access control on the CCO site

controls what software images a user account is allowed to download. Encryption using SSL protects the software images as they are being downloaded from the Cisco web server to the user's computer.

2.6.3 Installation of the TOE

The installation, generation and start up of the TOE such that it is in evaluated configuration are detailed in the Guidance documentation (Ref 2).

2.7 Version Verification

To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE component hardware models at the beginning of the PRE wrapper document (Ref 2). This document is made available on the Cisco website for download.

In addition to verifying model numbers for hardware components, the software versions must also be verified by the customer recipient. Software versions can be checked by following the "*Identifying the Evaluated Hardware and Software*" instruction included in the user guidance.

2.8 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. All guidance material is available for download at www.cisco.com. All common criteria guidance material is available at www.commoncriteriaportal.org. The Information Security Manual (ISM) is available at www.asd.gov.au.

2.9 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

TOE Environment Assumptions	
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation and testing as part of the evaluation.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the WLANPP (Ref 3) and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Refs 5 and 6).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 7).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Cisco WLAN Common Criteria Operational User Guidance and Preparative Procedures version-11 August 2016 (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the Evaluators were taken from the WLANPP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile were exercised during testing.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 8).

3.5 Penetration Testing

The Evaluators conducted independent and penetration testing between the 3rd July 2016 and the 2nd August 2016.

The Evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the Certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of WLAN access systems. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref 9) the Australasian Certification Authority **certifies** the evaluation of the Cisco WLAN 8.0 product performed by the Australasian Information Security Evaluation Facility, CSC Australia.

CSC Australia **has determined** that Cisco WLAN 8.0 upholds the claims made in the Security Target (Ref 1) and **has met** the requirements of WLANPP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the WLANPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 4) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled

b) Configure and operate the TOE according to the vendor’s product administrator guidance

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

h) Avoid the use of self signed certificates

i) Use the Command line interface (CLI) local console instead of the web GUI

j) Note that workstations used for remote administration of the TOE must be dedicated for performing administrative tasks on the TOE, and prevented from communicating (sending and receiving traffic) with assets not related to administration of the TOE.

k) Note that Internet Explorer is not compatible with the WLC WebGUI.

Annex A – References and Abbreviations

A.1 References

1. Cisco WLAN 8.0 Common Criteria Security Target, Version 1.0, September 2016

2. Guidance Documentation:

   - Cisco WLAN Common Criteria Operational User Guidance and Preparative Procedures version 0-11, August 2016.

3. U.S Government Protection Profile for Wireless Local Area Network (WLAN) Access Systems (WLANPP) Version 1.0, December 1, 2011

4. 2016 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components 09- 2012, Version 3.1 Revision 4

6. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components 09-2012, Version 3.1 Revision 4

7. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, 09- 2012, Version 3.1, Revision 4.

8. Entropy documentation

   - Cisco WLAN 8.0(APs) Entropy documentation 01 July 2014

   - Cisco WLAN Entropy Information Version 1.0 September 2016

9. Cisco WLAN 8.0, Evaluation Technical Report,(T0080) ,REFERENCE: CSC-EFC-T0080-ETR, EVALUATION-IN-CONFIDENCE, Version 1.0

10. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

11. NIST publication SP800-90B Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2016.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
AP	Access point
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WLC	Wireless LAN Controller