



Australian Government
Department of Defence

Australasian Information Security Evaluation Program

**Maintenance Report Supplementing
Certificate Report 2012/81**

**30 May 2013
Version 1.0**

Commonwealth of Australia 2013

Reproduction is authorised provided
that the report is copied in its entirety.

Amendment Record

Version	Date	Description
1.0	30/5/13	Public release

Table of Contents

1. Table of Contents.....	iv
2. Chapter 1 – Introduction.....	1
<i>1.1: Purpose.....</i>	<i>1</i>
<i>1.2: Identification</i>	<i>1</i>
3. Chapter 2 – IAR Summary.....	3
<i>2.1: Description of changes.....</i>	<i>3</i>

Chapter 1 – Introduction

1.1: Purpose

This document is an addendum to the Certification Report (Ref [1]) that describes the relevant baseline evaluation of the Cisco Wireless Local Area Network and Wireless Intrusion Prevention System.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Cisco for the Cisco Wireless Local Area Network and Wireless Intrusion Prevention System against the requirements contained in the Assurance Continuity: CCRA Requirements (Ref [2]).

Cisco provided information about their assurance continuity activities in the form of an Impact Analysis Report (IAR). The IAR (Ref [3]) list the changes made to the certified TOE, the evidence updated as the result of the changes and the security impact of the changes.

This report should be read in conjunction with:

- a) The certified TOE's Certification Report (Ref [1]).
- b) The certified TOE's Security Target v1.1 which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.
- c) The new Security Target version 2.1. (Ref [4]) which includes the updated version numbers. The scope has not changed.

1.2: Identification

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
Maintained TOE	Cisco Wireless LAN and Intrusion Prevention System v 7.0.240.0
Developer	Cisco Systems
Certified TOE	Cisco Wireless LAN and Intrusion Prevention System v 7.0.230.0
Security Target	Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target Version: 1.1 March 2013
Updated Security Target	Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security

	Target ,Version: 2.1, April 2013
Certificate Number	2012/81

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 of the Security Target (Ref [4]).

Chapter 2 – IAR Summary

2.1: Description of changes

The Impact Analysis Report (IAR) indicated that the following minor changes have been made to the Cisco WLAN and wIPS.

Table 2: Model Changes

Certified version	Changed version
7.0.230.0	7.0.240.0

The overall impact of the bug fixes is minor. In the changes from WLAN 7.0.230.0 to 7.0.240.0 minor bug fixes were applied. WLAN is built from millions of lines of code; the bug fixes applied to the software affect only a small fraction of that source code. Each fix was applied to make the TOE function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

Types of minor bug fixes that are not related to the TSF include:

- Changes only applicable to hardware models outside the TOE.
- Changes only applicable to features outside the TSF such as HREAP.
- Changes that resolve issues related to functionality outside the TSF, such as performance, and system availability.

Types of minor bug fixes that are related to the TSF include fixes related to:

- Functionality inside the TSF, but related to performance or availability of the TSF-related functionality such as remote management interfaces, or logging.
- Cryptographic functions inside the TSF such as entropy, random number generation.
- Protocol negotiation for protocols inside the TSF such as 802.11w (management frame protection), and EAP.

To provide assurance that none of the changes had any direct impact to evaluated functionality, Cisco re-ran for this Assurance Maintenance effort the entire set of test cases from the original EAL4 Common Criteria evaluation.

2.2 Documentation Updated:

The updated Security Target is 'Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target Version: 2.1 April 2013.'

Chapter 3 - Assurance Continuity

3.1 Assurance Continuity Result

After consideration of the Impact Analysis Report (IAR) provided by Cisco Systems, Australasian Certification Authority (ACA) has determined that the proposed changes are minor. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is maintained for Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) version 7.0.240.0.

References and Abbreviations

A.1 References

1. Certification Report 2012/81, Australasian Certification Authority.
2. Assurance Continuity: CCRA requirements, Common Criteria Interpretation Management Board, CCIMB-2004-02-009, Version 1.0, February 2004.
3. Impact Analysis Report: Cisco_WLAN7-0_EAL4_IAR_20130331
4. Cisco Wireless Local Area Network (WLAN) Access System with Integrated Wireless Intrusion Prevention System (wIPS) Security Target Version: 2.1 April 2013

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
HREAP	Hybrid Remote Edge Access Point
IAR	Impact Analysis Report
TOE	Target of Evaluation
TSF	TOE Security Function