SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-011 CR Certification Report

Issue 1.0 14 December 2009

AirMagnet Enterprise System 8.5

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.0 13.09.2007

SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY

Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Contents

1 Certification Statement

AirMagnet Enterprise System is a wireless intrusion detection system that provide a distributed wireless security and integrity management system.

AirMagnet Enterprise System 8.5 software version 8.5.0-12047 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 for the specified Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier Arne H. Rage
Quality Assurance	Lars Borgos Quality Manager Lars Borgos
Approved	Kjell W. Bergan Scheme Director Kjell W. Bergan
Date approved	14 December 2009

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
IDS	Intrusion Detection System
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[Add/remove/update as necessary]

[1] AirMagnet Enterprise System 8.5 Security Target, version 0.04 May2009

[2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.

[3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.

[4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.

[5] The Norwegian Certification Scheme, SD001E, Version 7.0, 28.03.2008.

[6] Common Methodology for Information Technology Security Evaluation, EvaluationMethodology, CCMB-2005-08-004, Version 2.3, August 2005.

[7] Evaluation Technical Report of the AirMagnet Enterprise System 8.5, software version 8.5.0-12047, Issue 1.1, 11 December 2009.

[8] AirMagnet Enterprise 8.5 User Guide, PrintUserGuide.pdf, August 19 2009.

[9] AirMagnet Delivery, Installation, Generation, and Start-up Procedures, AM_ADO.doc version 0.02.

[10] AirMagnet Enterprise 8.5 WLAN Policy Reference Guide, Policy_Reference_Guide.pdf, December 8 2008.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of AirMagnet Enterprise System 8.5 software version 8.5.0-12047 to the Sponsor, AirMagnet Inc, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was AirMagnet Enterprise System 8.5, software version 8.5.0-12047.

This product is also described in this report as the Target of Evaluation (TOE). The developer was AirMagnet Inc.

The TOE is a wireless intrusion detection system (IDS) and provides a distributed wireless security and integrity management system.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The AirMagnet Enterprise System 8.5 consists of three major components— SmartEdge Sensors that provide remote monitoring and troubleshooting of 802.11 wireless networks, a centralized Enterprise Server that correlates events and integrates to other systems, and Enterprise Console that provides the user interface to the system.

The TOE includes four Sensor models: AirMagnet SmartEdge Sensors A5020, A5120, A5023, and A5123.

4.4 Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. Predefined evaluation assurance level EAL 2 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].

4.6 Strength of Function

The minimum Strength of Function (SoF) was SoF-Basic. FIA_UAU.1 in the ST [1] includes the probabilistic/permutational mechanism in the form of password-based authentication of users, for which specific SoF metrics are appropriate

The cryptographic mechanism contained in the TOE is publicly known and as such it is the policy of SERTIT not to comment on its appropriateness or strength.

However, AirMagnet Sensors and Enterprise Server comply with FIPS 140-2 when performing FIPS approved cryptographic functions in the FIPS approved mode of operation. The modules have an overall rating of Level 2 and Level 1 respectively.

4.7 Security Policy

The TOE security policies are detailed in the ST [1].

4.8 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats, OSP's and assumptions which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products.

4.9 Threats Countered

The threats countered by the TOE and the TOE environment are as follows:

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.

- Improper security configuration settings may exist in the IT System the TOE monitors.
- Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
- Vulnerabilities may exist in the IT System the TOE monitors.
- The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
- The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
- The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
- Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
- Inadvertent activity and access may occur on an IT System the TOE monitors.
- Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

4.12 TOE Security Objectives

- The TOE shall provide cryptographic functions to maintain the confidentiality and allow for detection of modification of user data that is transmitted between physically separated portions of the TOE.
- The TOE will use NIST FIPS 140-1/2 certified crypto modules for cryptographic services implementing NIST-approved security functions and random number generation services used by cryptographic functions.
- The TOE must protect itself from unauthorized modifications and access to its functions and data.
- The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
- The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.
- The TOE must accept data from Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
- The TOE must respond appropriately to analytical conclusions.
- The TOE must include a set of functions that allow effective management of its functions and data.
- The TOE must allow authorized users to access only appropriate TOE functions and data.
- The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
- The TOE must appropriately handle potential audit and System data storage overflows.
- The TOE must record audit records for data accesses and use of the System functions.
- The TOE must ensure the integrity of all audit and System data.
- When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the System data.

4.13 Environmental Security Objectives

- Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
- Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

- Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
- Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
- The TOE is interoperable with the IT System it monitors.
- The TOE IT environment shall provide reliable time stamps to the TOE.
- The environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

4.14 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs)(Explicit requirements are indicated with the "EXP"):

FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected audit trail storage
FCS_BCM_EXP.1	Baseline Cryptographic Module
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP_EXP.1	Random Number Generation
FCS_COP_EXP.2(1)	Cryptographic Operation
FCS_COP_EXP.2(2)	Cryptographic Operation
FIA_ATD.1	Administrator attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.2	Secure security attributes
FMT_MTD.1(1)	Management of System and audit data
FMT_MTD.1(2)	Management of time data
FMT_SMF.1(1)	Specification of Management Functions (System and audit data)
FMT_SMF.1(2)	Specification of Management Functions (time data and security configuration management)
FMT_SMR.1	Security roles
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_ITT.1	Basic internal TSF data transfer protection

FPT_RVM.1(1)	Non-bypassability of the TOE Security Policy (TSP)
FPT_SEP.1(1)	TSF domain separation
FPT_STM_EXP.1	Reliable time stamps
IDS_ANL_EXP.1	Analyzer analysis
IDS_RCT_EXP.1	Analyzer react
IDS_RDR_EXP.1	Restricted Data Review
IDS_SDC_EXP.1	System Data Collection
IDS_STG_EXP.1	Guarantee of System Data Availability

4.15 Security Function Policy

The security policies that apply for the TOE are detailed in the ST [1] chapter 3.3.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001 [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation which was carried out by the evaluation facility Secode Norge AS (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT in 01.09.2009. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been comprised in delivery. Details can be found in AirMagnet Delivery, Installation, Generation, and Start-up Procedures [9].

5.3 Installation and Guidance Documentation

The guidance documents describes administrative functions and interfaces and how to administer the TOE in a secure manner and the functions and interfaces available to non-administrative users and the use of these functions. The guidance documents contain:

- warnings about functions and privileges that should be controlled in a secure processing environment
- assumptions regarding user behaviour
- security parameters under the control of the administrator
- security-relevant events
- IT environment requirements relevant to the administrator
- warnings about user-accessible security functions and privileges that should be controlled in a secure processing environment
- a presentation of all user responsibilities necessary for secure operation of the TOE
- IT environment requirements relevant to the user.

The guidance documents are AirMagnet Enterprise 8.5 User Guide [8] and AirMagnet Enterprise 8.5 WLAN Policy Reference Guide [10].

5.4 Vulnerability Analysis

The evaluators were satisfied that all obvious vulnerabilities are described, and a rationale is given for why it is/is not exploitable in the intended environment for the TOE, and that the vulnerability analysis is consistent with the ST and the guidance documents for the TOE. The evaluators also determined that the developer's search for TOE vulnerabilities is systematic.

The evaluators produced and conducted 4 penetration tests based on the developers' vulnerability analysis and information learned during penetration testing.

The tests validated the developer's conclusions.

The evaluator test team has not found any exploitable vulnerability or any residual vulnerability.

5.5 Developer's Tests

The developer has thoroughly tested all security functions of the TOE and the tests are divided in the following parts:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- IDS Function
- Cryptographic Support.

All together 56 tests are performed.

5.6 Evaluators' Tests

The evaluation team decided to focus the testing on the following security functions for devised testing:

- Security Audit
- Identification and Authentication
- Security Management
- IDS Function

The only security functions not selected for devised testing are Protection of the TSF and Cryptographic Support. These two security functions were the tested in the sample testing.

The evaluators have tested a sample of 46 tests of the developer's tests and verified expected and actual results.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that AirMagnet Enterprise System version 8.5 meets Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

The minimum Strength of Function was SoF-Basic.

SERTIT has also determined that the TOE meets the minimum SoF claim for FIA_UAU.1 of SoF-Basic given above under Section 3.6 "Strength of Function Claims".

6.2 Recommendations

Prospective consumers of AirMagnet Enterprise System version 8.5 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

AirMagnet Enterprise System 8.5 with software version 8.5.0-12047.

The AirMagnet Enterprise System 8.5 consists of three major components— SmartEdge Sensors that provide remote monitoring and troubleshooting of 802.11 wireless networks, a centralized Enterprise Server that correlates events and integrates to other systems, and Enterprise Console that provides the user interface to the system.

The SmartEdge Sensors included in this evaluation are A5020, A5120, A5023, and A5123.

TOE Documentation

The supporting guidance documents evaluated were:

- AirMagnet Enterprise System 8.5 Security Target [1]
- AirMagnet Enterprise 8.5 User Guide [8]
- AirMagnet Delivery, Installation, generation, and start-up procedures [9]
- AirMagnet Enterprise 8.5 WLAN Policy Reference Guide [10]

TOE Configuration

The following configuration was used for testing:

AirMagnet Server (Enterprise 8.5) and SQL (SQL-AME) are installed on Windows Server 2003 SE SP2. Console is installed on Windows XP SP3. Sensors are A5120 (indoor with spectrum) and A5123 (outdoor with spectrum).

The features related to Protection of the TSF and Cryptographic Support functions are tested using Wireshark (version 1.0.6).

For penetration testing of the AirMagnet Enterprise System 8.5, the following software was used from a PC running Windows XP SP3:

- Nmap version 4.90RC1
- Nessus version 4.0.1

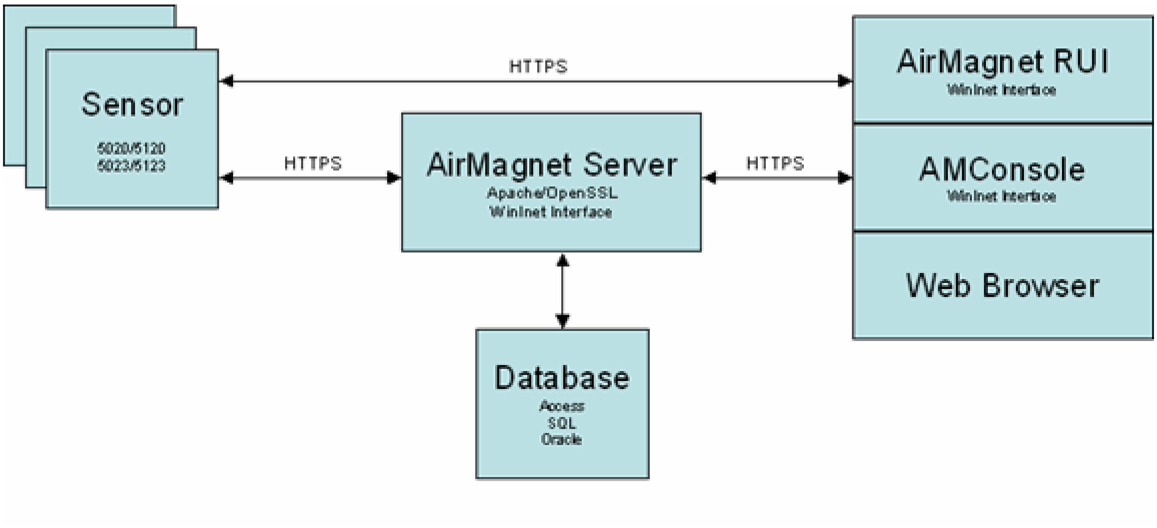

Figure 1 Test environment

The AirMagnet evaluator test environment is near fully-distributed. Server and Console are installed on separate computers and database components are installed on the computer with Server installed, that is SQL Configuration (scenario 2 from figure 3-1 in AirMagnet Enterprise 8.5 User Guide [8]).

Environmental Configuration

The AirMagnet Enterprise 8.5 consists of three major components— SmartEdge Sensors that provide remote monitoring and troubleshooting of 802.11 wireless networks, a centralized Enterprise Server that correlates events and integrates to other systems, and Enterprise Console that provides the user interface to the system.

As depicted on Figure 1, standalone SmartEdge Sensors (A5020, A5120, A5023, and A5123) are deployed near clusters of access points. The sensors provide security assessment, performance monitoring, network fault detection and remote troubleshooting functions. Administrators can monitor the security measures in use on every wireless network station and access point device to insure compliance with established policies, and also automatically scan for dozens of wireless network attacks.

Annex B: Product Security Architecture

This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

The intelligent sensors of AirMagnet Enterprise 8.5 provide around-the-clock coverage of the entire wireless environment including all 802.11a, 802.11b, and 802.11g channels and infrastructure. Each individual sensor includes the AirWISE Analytical Engine that, in real time, monitors and analyzes the security, performance, and reliability of the wireless network.

AirMagnet Sensors audit and validate the security of every Wi-Fi device in the network, helping to insure all users employ the appropriate level of security. Supported protocols include wep, leap, peap, tkip, mic, 802.1x, ttls, tls, wpa, pptp vpn, l2tp vpn, ssh vpn, ipsec vpn.

AirMagnet Enterprise is engineered to counter wireless threats - scanning the environment for Rogue APs and War-Drivers, Spoofed MAC Addresses, and a host of Denial of Service Attacks unique to Wi-Fi. Sensors send encrypted alarms in real time in response to an attack, allowing the staff to respond before network operations are negatively impacted. AirMagnet Sensors constantly monitor and generate alarms on over 20 key indicators of network health, allowing the administrators to take a proactive approach toward the maintenance of the network.

IT Personnel is allowed to tune sensor thresholds appropriately. Additionally, AirMagnet Enterprise supports unique user levels, insuring that the users access only the level of information appropriate for their role and level of responsibility.