National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Wireless (1100, 1200, 1300, 1400, 3200), Cisco Devices (IAD 2430), Cisco Access Servers (5350, 5400, 5850), and Cisco Secure Access Control Server (ACS) for Windows Server version 4.1.4.13

Report Number: **CCEVS-VR-VID6013-2008**
Dated: **June 9, 2008**
Version: **0.5**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20878

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95124-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory
Maria Tadeo
Ken Dill
.

Validation Personnel:
Robin Medlock, The MITRE Corporation
Jandria Alexander, The Aerospace Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Wireless (1100, 1200, 1300, 1400, 3200), Cisco Devices (IAD 2430), Cisco Access Servers (5350, 5400, 5850), and Cisco Secure Access Control Server (ACS) for Windows Server version 4.1.4.13. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Cisco Wireless and Cisco ACS was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during April 2008. The information in this report is largely derived from the Security Target (ST), written by Cisco Systems, Inc. and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product to be CC version 2.2 Part 2 and Part 3 conformant, including all Information Technology Security Evaluation Final Interpretations from January 2004 through March 25, 2004, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 3 augmented with Flaw Remediation (ALC_FLR.1) have been met.

The TOE is Cisco Systems Wireless (1100, 1200, 1300, 1400, 3200), Cisco Devices (IAD 2430), Cisco Access Servers (5350, 5400, 5850) running IOS and a Cisco Secure Access Control Server for Windows Server (ACS). These devices determine the next network point to which a packet should be forwarded toward its destination. They are located at any gateway (where one network meets another). They may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. IP packets are forwarded over one or more of its physical network interfaces to the device, which processes them according to the system's configuration and state information dynamically maintained by the device. This processing typically results in the IP packets being forwarded out of the device over another interface. The TOE also includes ACS, a software application that provides authentication, authorization, and accounting (AAA) services to network devices that function as AAA clients.

Devices that compose the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the devices (such as throughput and amount of storage) and therefore support security equivalency of the devices in terms of hardware:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operations
- Flash memory (EEPROM), used to store the IOS image (binary program)
- USB slot, used to connect USB devices to the TOE (not relevant as none of the USB devices are included in the TOE)
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store device configuration parameters used to initialize the system at startup.
- Physical network interfaces (minimally two). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces.

Figure 1 illustrates the TOE and its environment. The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the device or ACS Server are to be remotely administered, then the management station must be connected to a internal network, SSH must be used to connect to the device, and SSL must be used to connect to the ACS. The ACS, remote management, and NTP boxes (if used) must all be attached to the internal (trusted) network.

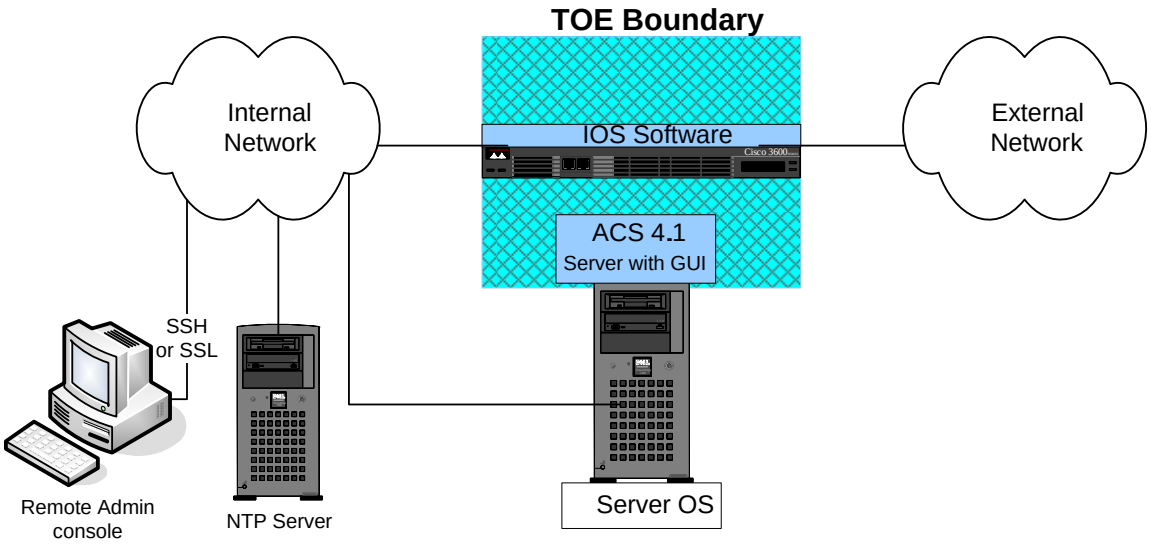

Figure 1: Typical TOE Configuration

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work unit verdicts), and reviewed successive versions of the ETR and test report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 3 augmented with ALC_FLR.1 evaluation. Therefore the validation team concludes that the Arca CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) 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) or candidate CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate 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 NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;

- 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
Target of Evaluation	Cisco Wireless (1100, 1200, 1300, 1400, 3200), Cisco Devices (IAD 2430), Cisco Access Servers (5350, 5400, 5850), and Cisco Secure Access Control Server (ACS) for Windows Server version 4.1.4.13
Security Target	Cisco Systems Wireless EAL3 Security Target Version 1.8 dated, April 24, 2008
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.7, released March 31, 2008. • ACM (Configuration Management Evaluation): ACM_CAP.3; ACM_SCP.1 Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.9, released March 31, 2008. • ALC (Life Cycle Evaluation): ALC_DVS.1; ALC_FLR.1; Evaluation Technical Report for Cisco Systems Wireless EAL3, document version 0.6, released March 31, 2008. • ADO (Delivery and Installation Evaluation): ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.8, released March 31, 2008. • ADV (Development Evaluation): ADV_FSP.1; ADV_HLD.2; ADV_RCR.1; Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.9 released May 15, 2008. • AGD (Administrative and User Guidance Evaluation): AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.9, released March 31, 2008. • ATE (Functional Testing, Testing Coverage, Testing Depth and Independent Testing Evaluation): ATE_COV.2; ATE_DPT.1, ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.7, released March 31, 2008. • AVA Vulnerability Assessment Evaluation): AVA_MSU.1; AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Cisco Systems Wireless EAL3, document Version 0.8, released March 31, 2008.
Protection Profile	None
Conformance Result	CC Part 2 and CC Part 3 conformant, EAL 3 augmented ALC_FLR.1
Applicable interpretations and precedents	▪ Compliant with all international interpretations with effective dates on or before February 25, 2004.

Item	Identifier
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95124-1706
Common Criteria Testing Lab (CCTL)	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validator(s)	Robin Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102 Jandria Alexander The Aerospace Corporation 6940 Columbia Gateway Drive Columbia, Maryland 21046

3 Security Policy

The TOE addresses the following features which are relevant to the secure configuration and operation of the device. ACS provides a modular way of performing Authentication, Authorization and Accounting.

3.1 Audit (Accounting)

The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Audited events include; modifications to the group of users that are part of the authorized administrator roles, all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the device or any failure of a packet to match an ACL rule allowing traffic to travel to or traverse of the device.

3.2 Identification & Authentication (Authentication)

Identification and Authentication provides the method of identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. The TOE performs authentication, using IOS platform authentication mechanisms, to authenticate access to user exec and privileged exec command modes.

Encryption of the packet body is provided through the use of Terminal Access Controller Access Control System (TACACS+) or RADIUS (note RADIUS only encrypts the password within the packet body). (TACACS+)is part of Authentication, Authorization, and Accounting (AAA) support. TACACS+ provides ACS-centralized user password authentication for all devices that the ACS manages and is an option that can be installed with ACS. Whenever a user requests some action, the device sends the user name and password to a central server located on the same server as the ACS. The server consults its access control database and either permits or denies the requested action.

3.3 Traffic Filtering

The TOE restricts remote terminal connectivity, using TOE platform access-control list functionality, to specific interfaces of the TOE so that sessions will only be accepted from the management station(s) identified in the management session TOE security policy.

Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the device's interfaces. The device examines each packet to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information. The device examines each packet to determine whether to forward or drop the packet, on the basis of the information contained within the routing tables.

3.4 Security Management / Access Control (Authorization)

The TOE allows authorized administrators to add new administrators; start-up and shutdown the device; create, modify, or delete configuration items; modify and set the time and date; and create, delete, empty, and review the audit trail. The ACS, when using TACACS+ or RADIUS, allows authentication administrators to modify and set the threshold for the number of permitted consecutive authentication attempt failures, and to restore authentication capabilities for users that have met or exceeded the threshold for permitted consecutive authentication attempt failures.

The TOE device platform maintains privileged and semi-privileged administrator roles. The device performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged modes.

3.5 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 privileged administrators. Additionally IOS is not a general purpose operating system and access to IOS memory space is restricted to only IOS functions.

The ACS component protects against interference and tampering by untrusted subjects through its own interfaces by implementing identification, authentication, and roles.

Both the device and ACS component ensure that when data is transmitted between them, security functions to protect the data from packet sniffing are invoked successfully before the data is transmitted.

The Cisco IOS contains a collection of features that build on the core components of the system. Those features that are not to be used include the HTTP Server, MAC address filtering, SNMP, Telnet, and VPN.

Apart from these exceptions, all types of network traffic through and to the TOE are within the scope of the evaluation.

4 Assumptions

The assumptions are ordered into three groups: Personnel Assumptions, Physical Environment Assumptions, and Operational Assumptions.

4.1.1 Personnel Assumptions

A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions

	provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
A.TRAIN_AUDIT	Administrators will be trained to periodically review audit logs to identify sources of concern
A.TRAIN_GUIDAN	Personnel will be trained in the appropriate use of the TOE to ensure security.

4.1.2 Physical Environment Assumptions

A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.1.3 Operational Assumptions

A.CONFIDENTIALITY	The hard copy documents that describe the configuration of the TOE, I&A information and Audit storage will be kept confidential and access will be limited to Authorized administrators.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.INTEROPERABILITY	The TOE will be able to function with the software and hardware of other device vendors on the network.
A.LOWEXP	The threat of malicious attacks aimed at exploiting the TOE is considered low.

5 Architectural Information

The TOE is the Cisco devices running IOS. The network on which they reside is part of the environment.

The following table lists the software, hardware and device operating system from Figure 1, below, and declares whether or not each is part of the TOE.

Table 2: TOE Boundary

HARDWARE	TOE?
Cisco network device (see table 3 below)	Yes
ACS Server hardware	No
OS	
Windows 2000 Server (ACS Server OS)	No
SOFTWARE	
Cisco ACS for Windows Server Version 4.1.4.13	Yes
TACACS+ or RADIUS[1]	Yes
IOS (see table 3 below)	Yes

Table 3: Evaluated Configurations

Series	Models	IOS Version	Type
1100	1100, 1130	12.3(8)JA2	Wireless
1200	1200, 1242AG	12.3(8)JA2	Wireless
1300	1300	12.3(8)JA2	Wireless
1400	1400	12.3(8)JA2	Wireless
3200	3270 or 3220 chassis with either one of 3230, or 3251 mobile wireless boards	12.4(6)XE3	Wireless Flexible, modular access routers
AS	AS5350, AS5400, AS5400HPX, AS5850	12.4(17)	Access Servers
IAD	IAD2430	12.4(17)	Integrated Access Device

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

[1] Software installed with ACS: Includes TACACS+ protocol as defined by Cisco Systems in draft 1.78 and RADIUS as specified in RFC 2865. The versions of TACACS+ and RADIUS are dependent upon ACS, so they are the same for all of the IOS versions included in the TOE.

Table 4: Evaluation Evidence

Component	Description
Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Wireless (ADM/IGS)	Version 0-15, March 2008
Cisco Systems IOS/AAA Functional Specification EAL3 Wireless (FSP)	Version 0-16, March 14, 2008
Cisco Systems IOS/AAA High Level Design EAL3 (HLD)	Version 0-14, January 30, 2008
Cisco's Configuration Management ,Plan and Delivery Procedures (CMP) Cisco AAA Configuration Items (CI)	Version 0.9, April 2007 Version 0-14 March 2008
Cisco Systems Vulnerability, Misuse and Strength of Function Wireless EAL3 (MSU_VLA_SOF)	Version 0-12, January 30, 2008
Cisco IOS Wireless EAL3 Detailed Test Plan (ATE)	Version 1.16 March 31, 2008
Cisco Systems Wireless EAL3 Security Target (ST)	Version 1.8 April 24, 2008

Guidance documentation is listed in Appendix A.1.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined each SFR and developed one or more Cisco test cases that verify the function or command requirement. These tests were documented in the Cisco IOS Wireless EAL3 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions.

The developer testing addresses the following security functionality claimed by the TOE: ssh communications, acl, demonstrates user lockout collaboration between the TOE device and ACS server, logging messages to the ACS server using Radius or TACACS+, syslog connections and also capabilities of the TOE to maintain audit records in the local buffer, ability of the AAA subsystem to authenticate users for console login using username/password configured locally on the device, attributes of a user and proving that a user cannot do any TSF mediated actions prior to identification and authentication, ability of administrators to carry out management functions, and traffic-filtering requirements.

See Appendices, device modules, identifies the individual modules that can compose the evaluated product.

The evaluation team determined that the developer's test methodology met the coverage and depth requirements and that the actual test results matched the expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer by creating a mapping of test cases to subsystem and SFR's.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested all TSF, and 24 SFRs.

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. The specific penetration tests executed include the following:

- Use a port scanner against the target network device to determine whether the target device may have different services listening on multiple TCP/IP-enabled interfaces and scanned each type of interface Checked for open ports on the target host/device.
- Test the different privilege levels and granting command access to the different levels.
- Test potential abuse privilege levels using the "autocommand" command.
- Checked for known vulnerabilities on the target host/device using nessus.
- Test potential misuse of the "kron" command to run commands as another user.

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

8 Evaluated Configuration

The evaluated configuration was tested in the configuration identified in Figure 2, below. The evaluation results are valid for all configurations of the TOE identified in section 4 of this report.

Figure 2: Testing Environment

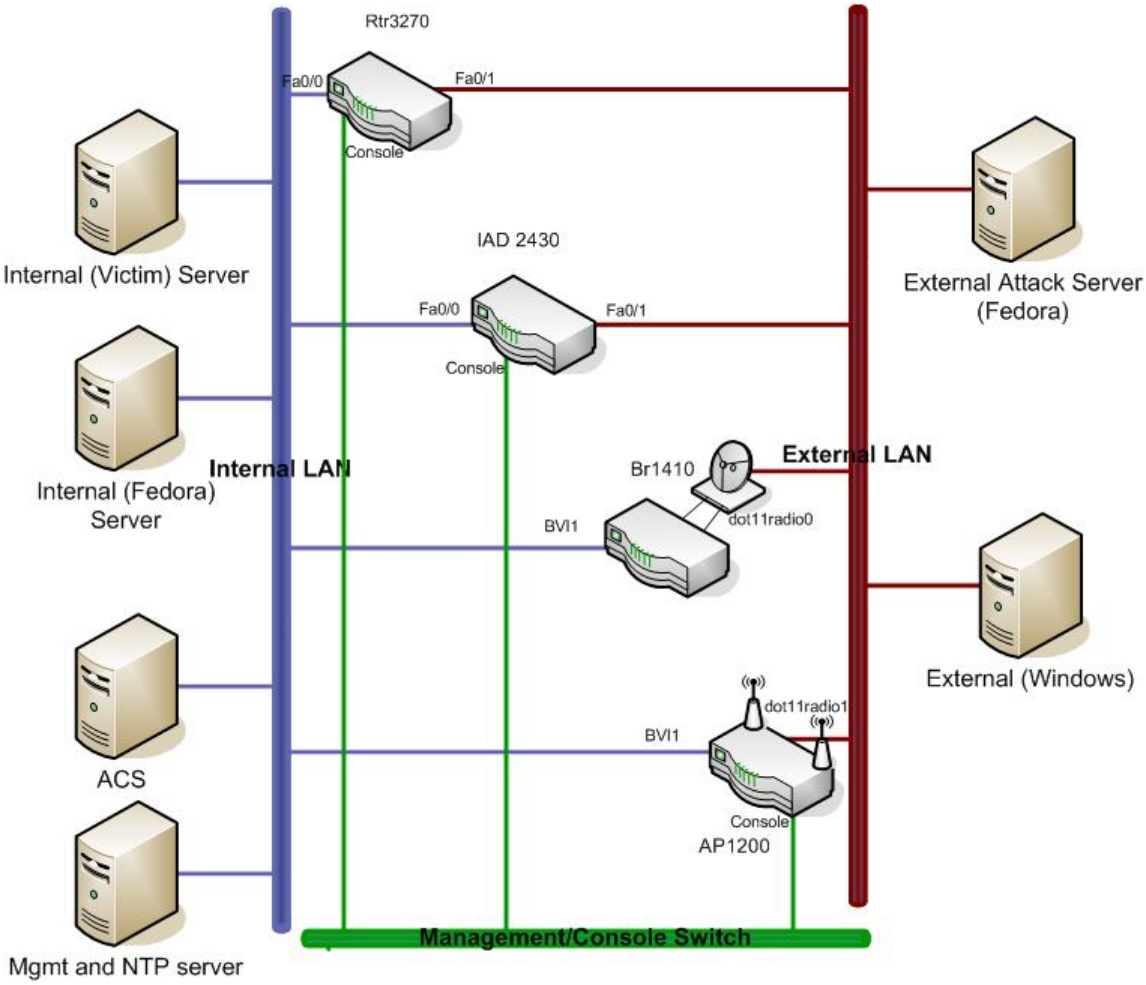

Table 5: Hardware and Software Components Tested

IOS Version	Models in TOE	Tested by CCTL
12.4(17)	AS5350 AS5400 AS5400HPX AS5850 IAD2430	IAD2430
12.3(8)JA2	1100, 1130 1200, 1232AG, 1242AG 1300 1400, 1410	1410 or 1200
12.4(6)XE3	3220 3230 3251 3270	3270 with 3230 boards

9 Validator Comments

The Validator has reviewed the evaluation technical report and agrees with the conclusion of this evaluation. The customer is reminded that the following were not included within the scope of the evaluation.

- There are no Protection Profile compliance claims
- The TOE does not address encryption (IPSec), VPNs, or Quality of Service (QoS)
- The TOE relies on the IT environment for the following:
  - Protected audit trail storage
  - Non-bypassability of the TSP
  - Partial environment TSF domain separation (this requirement is split between the TOE and the environment)
  - Reliable time stamps for the ACS component's use

10 Security Target

Cisco Systems Wireless EAL3 Security Target, Version 1.7, March 14, 2008.

11 List of Acronyms

ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CMS	Certificate Management System
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ID	Identifier
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
RFC	Request for Comment
SAR	Security Functional Requirement
SFR	Security Assurance Requirement
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target Of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
VR	Validation Report

12 Bibliography

The following documents referenced during preparation of the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

[7] Security Target for Cisco Systems Wireless EAL3, Version 1.8, April 24, 2008.

[8] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

[9] Cisco IOS Wireless EAL3 Detailed Test Plan Version 1.16, March 31, 2008

[10] Installation and Configuration for Common Criteria EAL3 Evaluated Cisco IOS/AAA Wireless, version 0-15, March 2008 .

13 Interpretations

13.1 International Interpretations

Official start date of the evaluation was February 25, 2004. The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied for this evaluation:

- The TOE is also compliant with all International interpretations with effective dates on or before Feb 25, 2004

13.2 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

- The TOE is also compliant with all International interpretations with effective dates on or before Feb 25, 2004

Appendix A.1 Guidance Documentation

The following is the list of other evaluation evidence provided by the sponsor:

Table 6: Guidance Documentation

- *Security Target for Cisco IOS/AAA Wireless, version 1.7*
- *Cisco IOS Security Configuration Guide, Release 12.4 (*http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a008043360a.html*)*
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.4 (*http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_book09186a0080430ee6.html*)*
- *Cisco IOS Security Configuration Guide, Release 12.3 (*http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html*)*
- *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 (*http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017d0a2.html*)*
- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2 (*http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ff9.html*)*
- *Cisco IOS Security Configuration Guide, Release 12.2 (*http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html*)*
- *Specific to IOS 12.3(8)JA2:*
    - *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA* (http://cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/configuration/guide/1238jasc.html)
    - *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.3(8)JA (*http://cisco.com/en/US/docs/wireless/access_point/12.3_8_JA/command/reference/1238jacr.html*)*
    - *Cisco IOS Software Configuration Guide for Cisco Aironet 1400 Series Wireless Bridge (12.3(8)JA) (*http://www.cisco.com/en/US/partner/docs/wireless/bridge/1400/12.3_8_JA/configuration/guide/sc1238ja.html*)*
- *Specific to IOS 12.4(6)XE3:*
    - *Cisco 3200 Series Mobile Access Router Software Configuration Guide (http://www.cisco.com/en/US/partner/products/hw/routers/ps272/products_configuration_guide_book09186a00800c7962.html)*
    - *Cisco IOS Command Reference for Cisco Access Points and Bridges (http://www.cisco.com/en/US/partner/products/hw/routers/ps272/products_technical_reference_book09186a008022da1f.html)*
- *Specific to IOS 12.4(17):*
    - *Cisco AS5300 Series Universal Gateways; AT Command Set and Register Summary for Cisco MICA Six-Port Modules (*http://www.cisco.com/en/US/products/hw/univgate/ps501/prod_command_reference09186a00800a97c9.html*)*

  - *Cisco AS5300 Software Configuration Guide (http://www.cisco.com/en/US/partner/products/hw/univgate/ps501/products_configuration_guide_book09186a008007dfbb.html)*
  - *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide (http://www.cisco.com/en/US/partner/docs/routers/access/as5350/software/configuration/guide/53swcg_1.html)*
  - *IOS Upgrades on the Cisco AS5800 (http://www.cisco.com/en/US/partner/products/hw/univgate/ps509/prod_configuration_guide09186a00800c98a3.html)*
  - *Cisco IOS Software Releases 12.4 Mainline Command References (http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html)*
  - *Cisco IOS Software Releases 12.4 Mainline Configuration Guides (http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html)*
  - *Cisco IAD2430 Series Integrated Access Devices Software Configuration Guide (http://www.cisco.com/en/US/partner/products/hw/gatecont/ps887/products_configuration_guide_book09186a0080192878.html)*
- *Installation Guide for Cisco Secure ACS for Windows, Release 4.1, Text Part Number: OL-9970-02 (http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/installation/guide/windows/IGwn41P.pdf)*
- *User Guide for Cisco Secure Access Control Server Release 4.1 , Text Part Number: OL-9971-01 (http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/ACSugP.pdf)*

Hardware Family	Installation Information
Access Servers	*Cisco AS5300 Quick Start Guide* *http://www.cisco.com/en/US/partner/products/hw/univgate/ps501/products_quick_start09186a00800a4* *7c.html* *Cisco AS5350 and Cisco AS5400 Universal Gateways Quick Start Guide* *http://www.cisco.com/en/US/partner/docs/routers/access/as5350/hardware/quick/guide/53_54QSG.htm* *Cisco AS5400 Universal Gateway Chassis Installation Guide* *http://www.cisco.com/en/US/partner/docs/routers/access/as5400/hardware/installation/guide/hwig.htm* *Cisco AS5800 Access Server Hardware Installation Guide* *http://www.cisco.com/en/US/partner/products/hw/univgate/ps509/products_installation_guide_book09* *6a008007cc9f.html*
Integrated Access Devices	*Cisco IAD2430 Series Integrated Access Device Hardware Installation Guide* *http://www.cisco.com/en/US/partner/products/hw/gatecont/ps887/products_installation_guide_book09* *6a00801d7e1d.html* *Cisco IAD2430 Series Integrated Access Devices -- Quick Start Guide* *http://www.cisco.com/en/US/partner/products/hw/gatecont/ps887/products_quick_start09186a008019* *91.html*
Wireless 1100 Series	*Quick Start Guide Cisco Aironet 1100 Series Access Points* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1100/quick/guide/ap11qsg.html* *Cisco Aironet 1100 Series Access Point Hardware Installation Guide, OL-4309-07* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1100/installation/guide/1100hig7.html* *Quick Start Guide Cisco Aironet 1130AG Access Point* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1130/quick/guide/ap1130qs.html* *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide, OL-8369-01* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1130/installation/guide/1130-TD-Book* *Wrapper.html*
Wireless 1200 Series	*Quick Start Guide Cisco Aironet 1200 Series Access Points Running Cisco IOS Software* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1200/ios/quick/guide/12iosqsg.html* *Cisco Aironet 1200 Series Access Point Hardware Installation Guide, OL-8370-04* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1200/installation/guide/1200-TD-Book* *Wrapper.html*
Wireless 1300 Series	*Quick Start Guide Cisco Aironet 1300 Series Outdoor Access Point* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1300/quick/guide/br13qsg.html* *Cisco Aironet 1300 Series Wireless Outdoor Access Point/Bridge Hardware Installation Guide, OL-5048-06* *http://www.cisco.com/en/US/partner/docs/wireless/access_point/1300/installation/guide/1300hig6.html*
Wireless 1400 Series	*Quick Start Guide Cisco Aironet 1400 Series Wireless Bridge* *http://www.cisco.com/en/US/partner/docs/wireless/bridge/1400/quick/guide/br1410qs.html* *Cisco Aironet 1400 Series Outdoor Bridge Hardware Installation Guide, OL-4072-04* *http://www.cisco.com/en/US/partner/docs/wireless/bridge/1400/installation/guide/1400hig4.html*

Hardware Family	Installation Information
Mobile Access Router 3200 Series	*Regulatory, Compliance, and Safety Information for the Cisco 3200 Mobile Access Router* *http://www.cisco.com/en/US/partner/products/hw/routers/ps272/products_regulatory_approvals_and_c* *mpliance09186a00804717b6.html* *Release Notes for the Cisco 3200 Series Routers for Cisco IOS Release 12.4(6)XE* *http://www.cisco.com/en/US/products/ps6706/prod_release_note09186a00806c23a8.html* *Cisco 3200 Series Router Hardware Reference* *http://www.cisco.com/en/US/partner/products/hw/routers/ps272/products_technical_reference_book09* *86a0080227b02.html* *Cisco 3200 Rugged Enclosure Assembly Guidelines* *http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/mar_assm/index.htm*