National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S

Report Number: CCEVS-VR-VID10760-2017

Dated: 11/21/2017

Version: 0.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick W. Mallett, MITRE, Lead Validator

Paul Bicknell, MITRE, Senior Validator

Common Criteria Testing Laboratory

Pascal Patin

Zalman Kuperman

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco IM&P Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in November 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the Collaborative Protection Profile for Network Devices (NDcPP) v 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work-units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the 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 evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance 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 Protection Profile(s) to which the product is conformant.
- 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
TOE	Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S
Protection Profile	Collaborative Protection Profile for Network Devices (NDcPP, v1.0)
Security Target	Cisco Unified Communications Manager IM and Presence Service (IM&P) 11.5SU3SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S, UCS C240 M4S Common Criteria Security Target
Evaluation Technical Report	Cisco IM&P Security Target Evaluation Technical Report, 10/16/17
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Patrick Mallett, Paul Bicknell

3 Architectural Information

The TOE is Cisco Unified Communications Manager IM and Presence Service running IM&P 11.5 (herein after referred to as IM&P). The TOE provides native standards-based, dual-protocol, enterprise instant messaging (IM) and network-based presence as part of Cisco Unified Communications capabilities.

IM&P is a hardware and software-based, native standards-based enterprise IM and network-based presence that is a part of Cisco Unified Communications family of products. IM&P is a secure and scalable service that offers users feature-rich communications capabilities within the enterprise as well as with external partners.

IM and Presence Service provides the foundation to deliver enterprise IM and network-based presence-enabled collaboration capabilities that allows users to view the presence status or availability of the people they want to communicate with, exchange instant messages with these individuals, and escalate to a voice and video call or a rich collaborative session.

The evaluated configuration of the TOE includes the IM&P 11.5 software installed on either the Cisco Unified Computing System™ (Cisco UCS) C220 M4S or C240 M4S Rack Server.

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

4.1.1 Security Audit

The Cisco IM&P provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco IM&P generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE audit event logging is centralized and enabled by default. Audit logs can be backed up over a secure TLS channel to an external audit server.

4.1.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; asymmetric key generation; cryptographic key establishment using RSA-based key establishment schemes and DH key establishment; digital signature using RSA; cryptographic hashing using SHA-256; random bit generation using DRBG and keyed-hash message authentication using HMAC-SHA (SHA-1, SHA-256, and SHA-384). The TOE implements the secure protocols TLS/HTTPS and TLS for the client and server. The algorithm certificate references are listed in the table below.

Algorithm	Description	Supported Mode	Cert. #	Module	SFR
RSA	Signature generation and Verification, and key generation and transport	FIPS PUB 186-4 Key Generation	#1743	FOM	FCS_CKM.1(1) FCS_COP.1(2)

Algorithm	Description	Supported Mode	Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	AES in CBC and GCM (128 and 256 bits)	#3404	FOM	FCS_COP.1(1)
SHS (SHA-1, 256, 384)	Cryptographic hashing services	Byte Oriented	#2817	FOM	FCS_COP.1(3)
HMAC SHA-1, SHA-256, SHA-384	Keyed hashing services and software integrity test	Byte Oriented	#2172	FOM	FCS_COP.1(4)
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	#817	FOM	FCS_RBG_EXT.1

CAVP Certificate References

The algorithm certificates applicable to the TOE are based on the underlying OS of the IM&P, which is RHEL 6/Linux kernel 2.6 with the Intel Xeon processor.

The TOE provides cryptography in support of remote administrative management via HTTPS. The TOE can also use the X.509v3 certificate for securing TLS sessions.

4.1.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection.

4.1.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- the configuration of the TOE;

- the configuration of access banners;
- the configuration of session inactivity;
- the verification and installation of TOE updates;
- the auditing behavior; and
- the cryptographic functionality

The TOE supports the security administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

4.1.5 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 Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IM&P is not a general-purpose operating system and access to Cisco IM&P memory space is restricted to only Cisco IM&P functions.

The TOE initially synchronizes time with the Cisco Unified Communications Manager that maintains and synchronizes with an NTP server and then internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.1.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE.

4.1.7 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over HTTPS and initiates secure HTTPS connections to transmit audit messages to remote syslog servers.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (NDcPP)

That information has not been reproduced here and the NDcPP should be consulted if there is interest in that material.

5.2 Threats

Likewise, the Security Problem Definition, including the threats, may be found in the NDcPP

The NDcPP should be consulted if there is need to review that material.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Unified Communications Manager IM and Presence Service (IM&P) Common Criteria Security Target v1.0
- Cisco Unified Communications Manager IM and Presence Service (IM&P) Common Criteria Configuration Guide v1.0

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration of the TOE is clearly identified in the Security Target.

7.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 1 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the TOE	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices Version 1.0.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco IM&P, which is not publically available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined Cisco IM&P to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP v 1.0.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by Cisco IM&P that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP v 1.0.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the

Assurance Activities specified in the NDcPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDcPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDcPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration instructions provided in the Configuration Guide documentation listed above to ensure the evaluated configuration is established and maintained.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality, including the Excluded Functionality discussed above, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated version of the products utilizes Cisco FIPS Object Module v6.0 crypto software and the Intel Xeon E5-2600 v4/E5-2600 v3 hardware/processors and no earlier or later versions were evaluated and therefore cannot be considered as compliant.

The TOE stores a limited amount of audit records in its internal persistent storage. It is recommended that the administrator configure the TOE to export audit logs to a remote audit storage server.

11 Annexes

Not applicable.

12 Security Target

Cisco Unified Communications Manager IM and Presence Service (IM & P)11.5SU3 running on Cisco Unified Computing System™ (Cisco UCS) C220 M4S and UCS C240 M4S Common Criteria Security Target v1.0

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.