National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Network Device Protection Profile (NDPP) Extended Package SIP Server, Version 1.1, November 5th 2014

Report Number: CCEVS-VR-PP-0022
Dated: 28 October 2015
Version: 1.0

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

Common Criteria Testing Laboratory

Base and Additional Requirements
Acumen Security, LLC.
Montgomery Village, Maryland

Table of Contents

1 Executive Summary 1
2 Identification 1
3 SIPEP Description 2
4 Security Problem Description and Objectives 3
4.1 Assumptions 3
4.2 Threats 3
4.3 Organizational Security Policies 4
4.4 Security Objectives 4
5 Requirements 5
6 Assurance Requirements 5
7 Results of the evaluation 5
8 Glossary 6
9 Bibliography 6

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Network Device Protection Profile (NDPP) Extended Package SIP Server, Version 1.1 (SIPEP11). It presents a summary of the SIPEP11 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the SIPEP11 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Cisco Unified Communications Manager 11.0. The evaluation was performed by the Acumen Security LLC., Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, United States of America, and was completed in August 2015. This evaluation addressed the base and additional requirements of the SIPEP11. Since the SIPEP is an extended package of the Network Device Protection Profile (NDPP), this evaluation also included requirements from this PP, although this is outside the scope of this VR.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the Acumen Security LLC., CCTL. Additional review of the PP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the SIPEP11 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP 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). Because the ST contains material drawn directly from the SIPEP11, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation. Note that the ST also contains materials from the base NDPP that the SIPEP11 is an extension of. Items in the ST that were taken from the base NDPP and do not relate to the SIPEP11 were not examined for this VR.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the SIPEP11 meets the requirements of the APE components. These findings were confirmed by the VR author. 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 and Technology (NIST) 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 interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the SIPEP11 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Cisco Unified Communications Manager 11.0, provided by Cisco Systems. The evaluation was performed by the Acumen Security LLC. Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, United States of America, and was completed in August 2015.

The SIPEP11 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are conditionally expected to be included if conformant TOEs provide that capability. The vendor may choose to include such requirements in the ST and still claim conformance to this EP. Since the SIPEP11 is an extended package of the NDPP, the ST and TOE must also claim conformance to the "base" NDPP, which includes any applicable optional requirements from that PP.

The EP's optional requirements may not be included in a particular ST; however, the initial evaluation that was performed (and subsequently used as a basis for this VR) included the optional requirements; therefore, the VR has been written with respect to both the base and additional requirements of the EP.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the SIPEP11.

Protection Profile	*Network Device Protection Profile (NDPP) Extended Package SIP Server, Version 1.1, November 5th, 2014.*
ST (Base)	Cisco Unified Communications Manager Security Target, Version 1.0, August 2015
Evaluation Technical Report (Base)	Evaluation Technical Report for the Cisco Unified Communications Manager (CUCM) Version 2.0, June 6th, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Acumen Security, LLC., Montgomery Village, MD USA
CCEVS Validators (base)	Jean Petty, MITRE Corporation Luke Florer, Aerospace Corporation

3 SIPEP Description

This Extended Package (SIPEP11) describes the security requirements for a Session Initiation Protocol (SIP) Server and provides a minimal baseline set of requirements targeted at mitigating well defined threats. However, this EP is not complete in itself, but rather extends the Security Requirements for Network Devices protection profile (NDPP).

A compliant TOE will provide security functionality that addresses threats to itself. It must also protect communications between itself and a VoIP client (i.e., smartphone) or another SIP server by using a TLS protected channel. As a registrar server, the SIP server will require user/password authentication of the SIP user for SIP REGISTER. The protocols required by this PP make use of certificates so the SIP server must securely store certificates and private keys.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of 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.

4.2 Threats

The following table describes the threats that are defined for this EP.

Table 2: Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

Threat Name	Threat Definition
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

4.3 Organizational Security Policies

There are no organizational security policies defined by the EP.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

The following table contains objectives for the Operational Environment.

Table 6: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner

5 Requirements

As indicated above, requirements in the SIPEP11 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the Cisco evaluation activity referenced above. Within the table, SFRs that are formatted in **bold** refer to SFRs that were defined in the NDPP but were augmented or modified for the SIPEP. SFRs with no formatting refer to SFRs that did not exist at all in the NDPP or were significantly redefined.

Requirement Class	Requirement Component
FCS: Cryptographic Support	**FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)**
	FCS_TLS_EXT.1: Transport Level Security
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_SIPS_EXT.1: Session Initiation Protocol (SIP) Server
	FIA_X509_EXT.1: X509 Certificates
FMT: Security Management	**FMT_SMF.1: Specification of Management Functions**
FPT: Protection of the TSF	**FPT_TUD_EXT.1: Trusted Update**
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel

The following table contains the optional requirements contained in Appendix C and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). As stated previously, all optional requirements were assessed as part of the initial evaluation that was conducted alongside the review of this EP.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLS_EXT.1: Datagram Transport Level Security	

6 Assurance Requirements

Since the SIPEP11 is an extension of the NDPP, the evaluation laboratory performed the assurance activities for the NDPP in the course of this evaluation. The SIPEP11 contains no additional assurance requirements.

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass

APE_OBJ.2	Pass
APE_REQ.1	Pass

8 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 as interpreted by the supplemental guidance in the SIPEP Assurance Activities to determine whether or not the claims made are justified.
- **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.

9 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

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

[6] Acumen Security LLC, Validation Report for the *Cisco Unified Communications Manager (CUCM) 11.0*, August 25th 2015.

[7] Cisco Unified Communications Manager Security Target, Version 1.0, August 2015.

[8] Network Device Protection Profile (NDPP) Extended Package SIP Server, Version 1.1, November 5, 2014.