National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Functional Package for Secure Shell (SSH)

Version 1.0

2021-05-13

Report Number: CCEVS-VR-PP-0075
Dated: 22 February 2023
Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 PKG_SSH_V1.0 Description 3
4 Security Problem Description and Objectives 4
4.1 Assumptions 4
4.2 Threats 4
4.3 Organizational Security Policies 4
4.4 Security Objectives 4
5 Functional Requirements 5
6 Assurance Requirements 6
7 Results of the Evaluation 7
8 Glossary 8
9 Bibliography 9

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0). It presents a summary of the PKG_SSH_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the PKG_SSH_V1.0, concurrent with the first product evaluation against the Functional Package's (FP's) requirements. The evaluated product was Infinera Corporation Transcend Network Management System Server 18.10.3 (Infinera Server).

This evaluation addressed the base security functional requirements of the PKG_SSH_V1.0 as well as selection-based requirements. The Validation Report (VR) author independently performed an additional review of the FP as part of the completion of this VR, to confirm it meets the applicable APE requirements.

The evaluation determined the PKG_SSH_V1.0 is both Common Criteria Part 2 extended and Part 3 conformant. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the FP identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from the PKG_SSH_V1.0; completion of the ASE workunits satisfied the applicable APE workunits.

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

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) containing Evaluation Activities, which are interpretations of CEM workunits specific to the technology described in the FP.

To promote thoroughness and efficiency, the evaluation of the PKG_SSH_V1.0 was performed concurrent with the first product evaluation against the FP. In this case, the Target of Evaluation (TOE) for the first product was Infinera Server, performed by Gossamer Security Solutions in Columbia, Maryland.

The PKG_SSH_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains selection-based requirements. Selection-based requirements are those that must be included based upon the selections made in other requirements and the abilities of the TOE.

Because these discretionary requirements may not be included in a particular ST, the initial use of the FP will address (in terms of the FP evaluation), the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the PKG_SSH_V1.0 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the FP evaluated by this VR. It also includes supporting information from the initial product evaluation performed against the FP.

Protection Profile	Functional Package for Secure Shell (SSH), Version 1.0, 2021-05-13 (PKG_SSH_V1.0)
ST (Base)	Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, Version 1.5, 12/09/2022
Assurance Activity Report (Base)	Assurance Activity Report for Infinera Corporation Transcend Network Management System Server 18.10.3, Version 0.3, 12/09/22
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 extended; CC Part 3 conformant
CCTL	Gossamer Security Solutions Columbia, MD
CCEVS Validators	Sheldon Durrant Lauren Hardy Randy Heimann Linda Morrison Clare Parran Farid Ahmed Russell Fink Anne Gugel Michael Smeltzer Richard (Rip) Toren

3 PKG_SSH_V1.0 Description

The PKG_SSH_V1.0 defines functional requirements for implementation of the SSH protocol. As a functional package, PKG_SSH_V1.0 is intended to be a repeatable definition of functional requirements that can be referenced from multiple Protection Profiles to ensure a standardized implementation of the protocol across various technology types. Functional packages do not define their own separate assurance requirements; instead, these are inherited from the Protection Profiles to which the evaluated product claims conformance to.

In this evaluation, this package has appropriately combined with the Application Software PP to include selection-based requirements in accordance with the selections or assignments made.

4 Security Problem Description and Objectives

4.1 Assumptions

Functional packages do not define a separate security problem; the use of a functional package is to define requirements for functional capabilities. The assumptions that govern the use of a product are not affected by its SSH protocol implementation.

4.2 Threats

Functional packages do not define a separate security problem; the use of a functional package is to define requirements for functional capabilities. The behavior defined by the functional package is used to mitigate threats that are defined in the PPs that reference the package.

4.3 Organizational Security Policies

Functional packages do not define a separate security problem; the use of a functional package is to define requirements for functional capabilities. The organizational security policies that govern the use of a product are not affected by its SSH protocol implementation.

4.4 Security Objectives

There are no TOE objectives defined in this FP. The behavior defined by the functional package is used to implement security objectives that are defined in the PPs that reference the package.

5 Functional Requirements

As indicated above, requirements in the PKG_SSH_V1.0 are comprised of the "base" requirements and selection-based requirements. The following table contains the "base" requirements that were validated as part of the Infinera Server evaluation.

Table 1: Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_SSH_EXT.1: SSH Protocol	Infinera Server

The PKG_SSH_V1.0 does not define any optional requirements.

The following table contains the "**Selection-Based**" requirements contained in Appendix B of the FP, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE workunits and has indicated its verification through "Package Evaluation" or "Module Evaluation."

Table 2: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_SSHC_EXT.1: SSH Protocol – Client	Infinera Server
	FCS_SSHS_EXT.1: SSH Protocol - Server	Package Evaluation

The PKG_SSH_V1.0 does not define any optional requirements.

6 Assurance Requirements

There are no assurance requirements specific to this FP. A TOE that includes this FP is evaluated against the assurance requirements defined by the claimed Base-PP.

7 Results of the Evaluation

Note that for APE elements and workunits identical to ASE elements and workunits, the lab performed the APE workunits concurrent to the ASE workunits.

Table 3: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	Package Evaluation
APE_CCL.1	Pass	Package Evaluation
APE_SPD.1	N/A	N/A
APE_OBJ.1	N/A	N/A
APE_ECD.1	N/A	N/A
APE_REQ.1	Pass	Package Evaluation

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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the PKG_SSH_V1.0 Evaluation Activities to determine whether 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.
- **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 the CCEVS Validation Body uses that leads to the issuance 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 VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Functional Package for Secure Shell (SSH), Version 1.0, 2021-05-13.

[6] Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target, Version 1.5, 12/09/2022.

[7] Assurance Activity Report for Infinera Corporation Transcend Network Management System Server 18.10.3, Version 0.3, 12/09/22.