National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Protection Profile for General Purpose Operating Systems, Version 4.3, 2022-09-27

Report Number: CCEVS-VR-PP-0091
Dated: 19 April 2024
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
Lightship Security USA, Inc.
Baltimore, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for General Purpose Operating Systems, Version 4.3, 2022-09-27 (PP_OS_v4.3). It presents a summary of the PP_OS_v4.3 and the evaluation results.

Lightship Security USA, Inc. located in Baltimore, MD, performed the evaluation of PP_OS_v4.3 concurrent with the first product evaluation against the Protection Profile's (PP's) requirements. The evaluated product was Red Hat Enterprise Linux 9.0 EUS (Red Hat).

This evaluation addressed the base requirements of PP_OS_v4.3. The PP_OS_v4.3 also includes several optional, selection-based, and objective requirements. The TOE claimed some but not all of these requirements. Requirements that were not claimed by the TOE were evaluated separately as part of the completion of the APE assurance requirements of the Common Criteria.

The Validation Report (VR) author independently performed an additional review of the PP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined that PP_OS_v4.3 is both Common Criteria Part 2 extended and Part 3 extended. An accredited CCTL evaluated PP_OS_v4.3, which is identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as well as additional scheme guidance required by NIAP. The Security Target (ST) includes material from PP_OS_v4.3. Only the portions of the ST evaluation that relate to PP_OS_v4.3 have been considered for this VR.

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 PPs that have Evaluation Activities, which are interpretations of CEM work units specific to the technology described by the PP.

To promote thoroughness and efficiency, the evaluation of PP_OS_v4.3 was performed concurrent with the first product evaluation against the PP requirements. In this case the Target of Evaluation (TOE) was Red Hat, performed by Lightship Security USA, Inc. located in Baltimore, MD.

PP_OS_v4.3 has a set of base requirements that all conformant STs must include, and additionally contains optional, selection-based, and objective requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based on the selections made in the base requirements and the capabilities of the TOE. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

A specific ST may not include all non-base requirements, so the initial use of the PP addresses (in terms of the PP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against PP_OS_v4.3. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include references to this as additional evidence that the corresponding portions of PP_OS_v4.3 were evaluated.

The following identifies the PP subject of the evaluation or validation, as well as the supporting information from the evaluation performed against this PP.

Protection Profile	Protection Profile for General Purpose Operating Systems, Version 4.3, 2022-09-27
ST (Base)	Red Hat Enterprise Linux 9.0 EUS Security Target, Version 1.1, January 2024
Assurance Activity Report (Base)	Red Hat, Inc., Red Hat Enterprise Linux 9.0 EUS Assurance Activity Report, Version 0.4, January 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Lightship Security USA, Inc. Baltimore, MD

3 PP_OS_v4.3 Description

PP_OS_v4.3 specifies information security requirements for operating systems, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

An operating system in the context of this PP is software that manages computer hardware and software resources and provides common services for application programs. The hardware it manages may be physical or virtual.

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: Assumptions

Assumption Name	Assumption Definition
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

4.2 Threats

The following table shows the applicable threats.

Table 2: Threats

Threat Name	Threat Definition
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.

Threat Name	Threat Definition
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

4.3 Organizational Security Policies

This protection profile contains no organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
O.ACCOUNTABILITY	Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.
O.INTEGRITY	Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.

The following table contains security objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
OE.PLATFORM	The OS relies on being installed on trusted hardware.

Environmental Security Objective	Environmental Security Objective Definition
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
OE.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

5 Requirements

As indicated above, requirements in PP_OS_v4.3 are comprised of the "base" requirements and additional requirements that are strictly or conditionally optional. The following table shows the "base" requirements validated as part of the Red Hat evaluation activities referenced above.

The ST has added iteration names to two components, but the components themselves were otherwise unchanged.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
PP_OS_V4.3		
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_CKM.2: Cryptographic Key Establishment (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Red Hat Enterprise Linux 9.0 EUS
	FCS_COP.1/ENCRYPT: Cryptographic Operation – Encryption/Decryption (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_COP.1/HASH: Cryptographic Operation – Hashing (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_COP.1/SIGN: Cryptographic Operation – Signing (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_COP.1KEYHMAC: Cryptographic Operation – Keyed-Hash Message Authentication (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FCS_RBG_EXT.1: Random Bit Generation	Red Hat Enterprise Linux 9.0 EUS (Iterated as "/KCAPI" and "/OSSL"
	FCS_STO_EXT.1: Storage of Sensitive Data	Red Hat Enterprise Linux 9.0 EUS
FDP: User Data Protection	FDP_ACF_EXT.1: Access Controls for Protecting User Data	Red Hat Enterprise Linux 9.0 EUS
FMT: Security Management	FMT_MOF_EXT.1: Management of security functions behavior	Red Hat Enterprise Linux 9.0 EUS
	FMT_SMF_EXT.1: Specification of Management Functions	Red Hat Enterprise Linux 9.0 EUS

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_ACF_EXT.1: Access controls	Red Hat Enterprise Linux 9.0 EUS
	FPT_ASLR_EXT.1: Address Space Layout Randomization	Red Hat Enterprise Linux 9.0 EUS (Iterated as "/Xeon," "/z16," and "/Power10")
	FPT_SBOP_EXT.1: Stack Buffer Overflow Protection	Red Hat Enterprise Linux 9.0 EUS
	FPT_TST_EXT.1: Boot Integrity	Red Hat Enterprise Linux 9.0 EUS
	FPT_TUD_EXT.1: Trusted Update	Red Hat Enterprise Linux 9.0 EUS
	FPT_TUD_EXT.2: Trusted Update for Application Software	Red Hat Enterprise Linux 9.0 EUS
	FPT_W^X_EXT.1: Write XOR Execute Memory Pages	PP Evaluation – *note this was moved from mandatory to optional per NIAP TD0675*
FAU: Audit Data Generation	FAU_GEN.1: Audit Data Generation (Refined)	Red Hat Enterprise Linux 9.0 EUS
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FIA_UAU.5: Multiple Authentication Mechanisms (Refined)	Red Hat Enterprise Linux 9.0 EUS
	FIA_X509_EXT.1: X.509 Certificate Validation	Red Hat Enterprise Linux 9.0 EUS
	FIA_X509_EXT.2: X.509 Certificate Authentication	Red Hat Enterprise Linux 9.0 EUS
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted channel communication	Red Hat Enterprise Linux 9.0 EUS
	FTP_TRP.1: Trusted Path	Red Hat Enterprise Linux 9.0 EUS
PKG_TLS_V1.1		
FCS: Cryptographic Support	FCS_TLS_EXT.1: TLS Protocol	Red Hat Enterprise Linux 9.0 EUS
PKG_SSH_V1.0		
FCS: Cryptographic Support	FCS_SSH_EXT.1: SSH Protocol	Red Hat Enterprise Linux 9.0 EUS

The following table contains the "**Optional**" requirements included in Appendix A, 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 optional requirement, the VR author has evaluated it through the completion of the relevant APE workunits and has indicated its verification through "PP Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
PP_OS_V4.3 – Strictly Optional Requirements		
FTA: TOE Access	FTA_TAB.1: Default TOE access banners	Red Hat Enterprise Linux 9.0 EUS
PKG_TLS_V1.1 – Strictly Optional Requirements		
No strictly optional requirements in PKG_TLS_V1.1.		
PKG_SSH_V1.0 – Strictly Optional Requirements		
No strictly optional requirements in PKG_SSH_V1.0.		
PP_OS_V4.3 – Objective Requirements		
FPT: Protection of the TSF	FPT_BLT_EXT.1: Limitation of Bluetooth Profile Support	PP Evaluation
	FPT_SRP_EXT.1: Software Restriction Policies	Red Hat Enterprise Linux 9.0 EUS
PKG_TLS_V1.1 – Objective Requirements		
FCS: Cryptographic Support	FCS_TLSC_EXT.3: TLS Client Support for Signature Algorithms Extension	Red Hat Enterprise Linux 9.0 EUS
	FCS TLSS_EXT.3 : TLS Server Support for Signature Algorithms Extension	Package Evaluation
PKG_SSH_V1.0 – Objective Requirements		
No objective requirements in PKG_SSH_V1.0.		

The following table contains the "**Selection-Based**" requirements included in Appendix B, and an indication of what evaluation those requirements were verified in (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 "PP Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
PP_OS_V4.3		
FDP: User Data Protection	FDP_IFC_EXT.1: Information flow control	PP Evaluation
PKG_TLS_V1.1		
FCS: Cryptographic Support	FCS_TLSC_EXT.1: TLS Client Protocol	Red Hat Enterprise Linux 9.0 EUS
	FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication	Package Evaluation
	FCS_TLSC_EXT.4: TLS Client Support for Renegotiation	Package Evaluation
	FCS_TLSC_EXT.5: TLS Client Support for Supported Groups Extension	Red Hat Enterprise Linux 9.0 EUS
	FCS_TLSS_EXT.1: TLS Server Protocol	Package Evaluation

Requirement Class	Requirement Component	Verified By
	FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication	Package Evaluation
	FCS_TLSS_EXT.4: TLS Server Support for Renegotiation	Package Evaluation
	FCS_DTLSC_EXT.1: DTLS Client Protocol	Package Evaluation
	FCS_DTLSC_EXT.2: DTLS Client Support for Mutual Authentication	Package Evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol	Package Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Support for Mutual Authentication	Package Evaluation
PKG_SSH_V1.0		
FCS: Cryptographic Support	FCS_SSHC_EXT.1: SSH Protocol – Client	Red Hat Enterprise Linux 9.0 EUS
	FCS_SSHS_EXT.1: SSH Protocol – Server	Red Hat Enterprise Linux 9.0 EUS

6 Assurance Requirements

The following are the assurance requirements contained in PP_OS_v4.3.

Table 10: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance claims	Red Hat Enterprise Linux 9.0 EUS
	ASE_ECD.1: Extended components definition	Red Hat Enterprise Linux 9.0 EUS
	ASE_INT.1: ST Introduction	Red Hat Enterprise Linux 9.0 EUS
	ASE_OBJ.1: Security objectives for the operational environment	Red Hat Enterprise Linux 9.0 EUS
	ASE_REQ.1: Stated security requirements	Red Hat Enterprise Linux 9.0 EUS
	ASE_SPD.1: Security problem definition	Red Hat Enterprise Linux 9.0 EUS
	ASE_TSS.1: TOE summary specification	Red Hat Enterprise Linux 9.0 EUS
ADV: Development	ADV_FSP.1 Basic functional specification	Red Hat Enterprise Linux 9.0 EUS
AGD: Guidance Documents	AGD_OPE.1: Operational user guidance	Red Hat Enterprise Linux 9.0 EUS
	AGD_PRE.1: Preparative procedures	Red Hat Enterprise Linux 9.0 EUS
ALC: Life-cycle Support	ALC_CMC.1: Labelling of the TOE	Red Hat Enterprise Linux 9.0 EUS
	ALC_CMS.1: TOE CM coverage	Red Hat Enterprise Linux 9.0 EUS
	ALC_TSU_EXT.1: Timely security updates	Red Hat Enterprise Linux 9.0 EUS
ATE: Tests	ATE_IND.1: Independent Testing – conformance	Red Hat Enterprise Linux 9.0 EUS
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Red Hat Enterprise Linux 9.0 EUS

7 Results of the Evaluation

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

Table 11: Evaluation Results PP_OS_V4.3

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Red Hat Enterprise Linux 9.0 EUS
APE_ECD.1	Pass	Red Hat Enterprise Linux 9.0 EUS
APE_INT.1	Pass	Red Hat Enterprise Linux 9.0 EUS
APE_OBJ.2	Pass	Red Hat Enterprise Linux 9.0 EUS
APE_REQ.2	Pass	Red Hat Enterprise Linux 9.0 EUS
APE_SPD.1	Pass	Red Hat Enterprise Linux 9.0 EUS

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 PP_OS_v4.3 Assurance 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] Common Criteria Evaluation and Validation Scheme, Publication #3, *Guidance to Validators*, Version 4.0, February 2020.

[6] Protection Profile for General Purpose Operating Systems, Version 4.3, 2022-09-27

[7] Red Hat Enterprise Linux 9.0 EUS Security Target Version 1.1, January 2024