# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# for the

## Red Hat Enterprise Linux Version 8.1

## Version 1.0

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-VID11107-2021** |
| **Dated:** | **01/04/2021** |
| **Version:** | **0.1** |

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

**NIAP**
**NBP 220**
**2720 Technology Drive**
**Annapolis Junction, MD 20701**

# ACKNOWLEDGEMENTS

## Validation Team

*Sheldon Durrant,*

*John Butterworth*

## Common Criteria Testing Laboratory

*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 Red Hat Enterprise Linux 8.1 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 January 2021. 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 Extended, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP].

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. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the GPOSPP 4.2.1 & SSHEP 1.0. 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 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 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.

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE** | Red Hat Enterprise Linux 8.1 |
| **Protection Profile** | Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP] |
| **Security Target** | Red Hat Enterprise Linux 8.1 Security Target |
| **Evaluation Technical Report** | Red Hat Enterprise Linux 8.1 Evaluation Technical Report |
| **CC Version** | Version 3.1, Revision 5 |
| **Conformance Result** | CC Part 2 Extended and CC Part 3 Extended |
| **Sponsor** | Red Hat, Inc. |
| **Developer** | Red Hat, Inc. |
| **Common Criteria Testing Lab (CCTL)** | Acumen Security, LLC<br>2400 Research Blvd Suite #395<br>Rockville, MD 20850 |
| **CCEVS Validators** | Sheldon Durrant<br>John Butterworth |

**Table 1 Evaluation Identifiers**

# 3 Architectural Information

Red Hat® Enterprise Linux® is the world's leading enterprise Linux platform. It's an open source operating system (OS) that supports multiple users, user permissions, access controls, and cryptographic functionality.

# 4 Security Policy

### Security Audit

The TOE generates and stores audit events using the Lightweight Audit Framework (LAF). The LAF is designed to be an audit system making Linux compliant with the requirements from Common Criteria by intercepting all system calls and retrieving audit log entries from privileged user space applications. The framework allows configuring the events to be recorded from the set of all events that are possible to be audited. Each audit record contains the date and time of event, type of event, subject identity, user identity and results (success/fail) of the action if applicable.

## Cryptographic Support

The TOE provides a broad range of cryptographic support; providing SSHv2 and TLSv1.2 protocol implementations in addition to individual cryptographic algorithms.

The cryptographic services provided by the TOE are described below:

| Cryptographic Protocol | Use within the TOE |
|---|---|
| SSH Client | The TOE allows administrators and users to connect to remote SSH servers. |
| SSH Server | The TOE allows remote administrators to connect using SSH. |
| TLS Client | The TOE connects to remote trusted IT entities using TLS. |

**Table 2 TOE Cryptographic Protocols**

The TOE includes two cryptographic libraries/implementations. Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

| Algorithm | Related SFRs | TOE Use | CAVP Certificate # |
|---|---|---|---|
| OpenSSL v1.1.1c with algorithm version rhel8.20190624cc | | | |
| AES | FCS_COP.1(1)<br>FCS_COP.1(1)/SSH<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.1<br>FCS_STO_EXT.1 | SSH AES CBC and CTR modes with 128 and 256-bit keys<br>TLS AES CBC and GCM modes with 128 and 256-bit keys<br>File Encryption using AES CBC with 128 and 256-bit keys | A796 |
| Diffie-Hellman | FCS_CKM.2<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.1 | SSH Diffie-Hellman Group 14 Key Establishment<br>TLS Diffie-Hellman Group 14 Key Establishment | N/A |

| Algorithm | Related SFRs | TOE Use | CAVP Certificate # |
|---|---|---|---|
| DRBG | FCS_DRBG_EXT.1 | CTR_DRBG (AES-256) | A796 |
| ECDSA | FCS_CKM.1<br>FCS_COP.1(3)<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.1<br>FCS_TLSC_EXT.2<br>FCS_TLSC_EXT.4 | SSH ECDSA P-256 and P-384 Host Key and User Key Generation<br>SSH EC Diffie-Hellman P-256, P-384, and P-521 Key Generation<br>SSH ECDSA P-256 and P-384 Host and User Signature Generation and Verification<br>TLS ECDSA P-256, P-384, and P-521 Client Key Generation<br>TLS EC Diffie-Hellman P-256, P-384, and P-521 Key Generation<br>TLS ECDSA P-256, P-384, and P-521 Signature Generation and Verification | A796 |
| HMAC | FCS_COP.1(4)<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.1 | SSH HMAC-SHA-256 and HMAC-SHA-512<br>TLS HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384<br>TLS HMAC-SHA-256 and HMAC-SHA-384 Key Derivation | A796 |
| KAS | FCS_CKM.2<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.2 | SSH EC Diffie-Hellman P-256, P-384, and P-521 Key Establishment<br>TLS EC Diffie-Hellman P-256, P-384, and P-521 Key Establishment | A796 |
| RSA | FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1(3)<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1<br>FCS_TLSC_EXT.1<br>FCS_TLSC_EXT.4<br>FPT_TST_EXT.1<br>FPT_TUD_EXT.1<br>FPT_TUD_EXT.2 | SSH RSA 2048-bit, 3072-bit, and 4096-bit Host Key and User Key Generation<br>SSH RSA 2048-bit, 3072-bit, and 4096-bit Host and User Signature Generation and Verification<br>TLS RSA 2048-bit, 3072-bit, and 4096-bit Client Key Generation<br>TLS RSA 2048-bit, 3072-bit, and 4096-bit Key Establishment (CAVP certificate is N/A)<br>TLS RSA 2048-bit, 3072-bit, and 4096-bit Signature Generation and Verification<br>Self-Test RSA 2048 Signature Verification<br>Trusted Update RSA 4096 Signature Verification | A796 |

| Algorithm | Related SFRs | TOE Use | CAVP Certificate # |
|---|---|---|---|
| SHS | FCS_COP.1(2)<br>FCS_SSHC_EXT.1<br>FCS_SSHS_EXT.1 | SSH SHA-1, SHA-256, SHA-384, and SHA-512 Key Derivation<br>SHA-1, SHA-256, SHA-384, and SHA-512 for Digital Signatures and HMACs | A796 |

**Table 3 CAVP Algorithm Testing References**

The OpenSSL library provides the TLS Client function. The OpenSSL library also provides the cryptographic algorithms for the SSH Client, SSH Server, trusted update, and secure boot security functions.

### User Data Protection

Discretionary Access Control (DAC) allows the TOE to assign owners to file system objects and Inter-Process Communication (IPC) objects. The owners are allowed to modify Unix-type permission bits for these objects to permit or deny access for other users or groups. The DAC mechanism also ensures that untrusted users cannot tamper with the TOE mechanisms.

The TOE also implements POSIX Access Control Lists (ACLs) that allow the specification of the access to individual file system objects down to the granularity of a single user.

### Identification and Authentication

User identification and authentication in the TOE includes all forms of interactive login (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the su or sudo command. These all rely on explicit authentication information provided interactively by a user.

The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported.

Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

### Security Management

The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF.

### Protection of the TSF

The TOE implements self-protection mechanisms that protect the security mechanisms of the TOE as well as software executed by the TOE. The following self-protection mechanisms are implemented and enforced:

- Address Space Layout Randomization for user space code.

- Stack buffer overflow protection using stack canaries.
- Secure Boot ensuring that the boot chain up to and including the kernel together with the boot image (initramfs) is not tampered with.
- Updates to the operating system are only installed after their signatures have been successfully validated.
- Application Whitelisting restricts execution to known/trusted applications

### TOE Access

The TOE displays informative banners before users are allowed to establish a session.

### Trusted Path/Channels

The TOE supports TLSv1.2 and SSHv2 to secure remote communications.  Both protocols may be used for communications with remote IT entities. Remote administration is only supported using SSHv2.

# 5 Assumptions, Threats & Clarification of Scope

## 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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.

The following assumptions are drawn directly from the [GPOSPP]:

| ID | Assumption |
|---|---|
| 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. |

**Table 4 Assumptions**

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

The following threats are drawn directly from the [GPOSPP]:

| ID | Threat |
|---|---|
| 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. |
| 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. |

**Table 5 Threats**

## 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP].
- 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:

- Red Hat Enterprise Linux 8.1 CC Guidance, Version 1.4, dated December 2020

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices as described in Table 6 below:

| Component | Required | Usage/Purpose Description for TOE performance |
|---|---|---|
| Workstation with SSH Client | No | This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE users (including administrators) to remotely connect to the TOE through SSH protected channels. Any SSH client that supports SSHv2 may be used. |
| Audit Server | No | The audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. |
| Update Server | Yes | Provides the ability to check for updates to the TOE as well as providing signed updates. |

Table 6 IT Environment Components

## 7.2 Excluded Functionality

None

# 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 Red Hat Enterprise Linux 8.1, which is not publicly 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly 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 5 and CEM version 3.1 rev 5. The evaluation determined the Red Hat Enterprise Linux 8.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the [GPOSPP] and [SSHEP].

## 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 the Red Hat Enterprise Linux 8.1 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP].

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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP] 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP] 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP] 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP], 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP], 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Extended Package for Secure Shell (SSH), Version 1.0 [SSHEP], 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 TOE. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFRs within the Security Target was evaluated. All other functionality provided by the TOE, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

Red Hat Enterprise Linux 8.1 Security Target v0.6, December 2020

# 13 Glossary

The following definitions are used throughout this document:

No additional terms are defined.

# 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 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.