National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Red Hat Enterprise Linux 8.6

Report Number: CCEVS-VR-VID11309-2024

Dated: January 15, 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

Validation Team

Jim Donndelinger
Patrick Mallett, PhD
Dave Thompson

The Aerospace Corporation

Common Criteria Testing Laboratory

Elliot Keen

Chaitanya Muzumdar

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 8.6 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 2024. 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 U.S. Government Protection Profile for Security Requirements for General Purpose Operating Systems, Version 4.2.1 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0]

The 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 Protection Profile for General Purpose Operating Systems, Version 4.2.1 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0]. 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 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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	Red Hat Enterprise Linux 8.6
Protection Profile	Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP] and Functional Package for SSH Version 1.0[PKG_SSH]
Security Target	Red Hat Enterprise Linux 8.6 Security Target
Evaluation Technical Report	Evaluation Technical Report for Red Hat Enterprise Linux 8.6
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Red Hat, Inc.
Developer	Red Hat, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Jim Donndelinger, Patrick Mallett Dave Thompson of the Aerospace Corporation.

3 Architectural Information

Red Hat® Enterprise Linux® is an open-source operating system (OS) that supports multiple users, user permissions, access controls, and cryptographic functionality.

3.1 TOE Description

This section provides an overview of the TOE, including physical boundaries, security functions, and relevant TOE documentation and references.

3.1.1 Physical Boundaries

The TOE itself is an operating system which can be installed on any compatible hardware; as such, the TOE does not have physical boundaries. However, the TOE was evaluated on the following hardware:

Table 1 – Hardware Platforms

Vendor	Model	CPU
Dell Inc.	PowerEdge R440	Xeon Silver 42xx
Dell Inc.	PowerEdge R540	Xeon Silver 42xx
Dell Inc.	PowerEdge R640	Xeon Silver 42xx
Dell Inc.	PowerEdge R740	Xeon Silver 42xx
Dell Inc.	PowerEdge R740XD	Xeon Silver 42xx
Dell Inc.	PowerEdge R840	Xeon Silver 42xx
Dell Inc.	PowerEdge R940	Xeon Silver 42xx
Dell Inc.	PowerEdge R940xa	Xeon Silver 42xx
IBM	z15 8561-T01	IBM z15
IBM	z15 8562-T02	IBM z15
IBM	z15 8561-LT1	IBM z15
IBM	z15 8562-LT2	IBM z15

Dell Platforms:

The Xeon Silver 4200 series processors are 2nd Generation Intel® Xeon® Scalable Processors and implement the Cascade Lake microarchitecture.

The TOE was tested on a PowerEdge R740 with a Xeon Silver 4216 CPU.

IBM Platforms:

The TOE is one instance of RHEL 8 running on an abstract machine and has full control over the abstract machine inside an IBM z15 T01, T02, LT1, or LT2 mainframe (machine type 8561 or 8652). The abstract machine is provided by a logical partition of the z15 processor. The partition includes 5 IFL (Integrated Facility for Linux) processors. An IFL is a processor dedicated to and

optimized for Linux workloads. Because of SMT, the IFL's appear as 10 logical processors allocated to the partition.

The TOE was tested on an IBM z15 T01 mainframe (machine type 8561).

3.2 TOE Environment

The following components must be present in the operational environment to operate the TOE in the evaluated configuration:

Table 3 - Operational Environment Components

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.
Update Server	Yes	Provides the ability to check for updates to the TOE as well as providing signed updates.

4 Security Policy

The TOE provides the security functions required by PP_OS_V4.2.1 and PKG_SSH_V1.0.

4.1 Security Audit

The TOE generates and stores audit events locally using administrator defined rules.

4.2 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, and in full detail in Section 6.2 of this document.

Table 4 TOE Cryptographic Protocols

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.

The TOE includes the OpenSSL cryptographic library, and each cryptographic algorithm has been validated for conformance to the requirements specified in their respective standards as identified in Section 6.2 of the ST.

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.

The TOE also provides a kernel cryptographic API (KCAPI), which implements an SP 800-90A compliant HMAC_DRBG to generate high-security random output for key generation or seed material.

4.3 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.

4.4 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.

4.5 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.

4.6 TOE Access

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

4.7 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 kernel-space isolation and TSF self-protection mechanisms are implemented and enforced (full details are provided in the TSS):

- Address Space Layout Randomization for user space code.
- Kernel and user-space ring-based separation of processes
- Stack buffer overflow protection using stack canaries.
- Secure Boot ensures 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.

4.8 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.

ID	Description
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.

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.

ID	Description
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.

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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0]
- 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.
- Vulnerabilities identified by a search of known vulnerabilities at the time of evaluation completion have been mitigated through vendor patches to the TOE or by workarounds specified in the Guidance Documents. Users should heed the workarounds.
- 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 document was provided by the vendor with the TOE for evaluation:

- Red Hat Enterprise Linux 8.6 Common Criteria Guidance, v3.5 January 2024.

To use the product in the evaluated configuration, the product must be configured as specified in these guides. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download this CC configuration guide (CCECG above) from the NIAP website.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in section 6.

The TOE itself is an operating system which can be installed on any compatible hardware; as such, the TOE does not have physical boundaries. However, the TOE was evaluated on the following hardware:

Table 2 – Hardware Platforms

Vendor	Model	CPU
Dell Inc.	PowerEdge R440	Xeon Silver 42xx
Dell Inc.	PowerEdge R540	Xeon Silver 42xx
Dell Inc.	PowerEdge R640	Xeon Silver 42xx
Dell Inc.	PowerEdge R740	Xeon Silver 42xx
Dell Inc.	PowerEdge R740XD	Xeon Silver 42xx
Dell Inc.	PowerEdge R840	Xeon Silver 42xx
Dell Inc.	PowerEdge R940	Xeon Silver 42xx
Dell Inc.	PowerEdge R940xa	Xeon Silver 42xx
IBM	z15 8561-T01	IBM z15
IBM	z15 8562-T02	IBM z15
IBM	z15 8561-LT1	IBM z15
IBM	z15 8562-LT2	IBM z15

Dell Platforms:

The Xeon Silver 4200 series processors are 2nd Generation Intel® Xeon® Scalable Processors and implement the Cascade Lake microarchitecture.

The TOE was tested on a PowerEdge R740 with a Xeon Silver 4216 CPU.

IBM Platforms:

The TOE is one instance of RHEL 8 running on an abstract machine and has full control over the abstract machine inside an IBM z15 T01, T02, LT1, or LT2 mainframe (machine type 8561 or 8652). The abstract machine is provided by a logical partition of the z15 processor. The partition includes 5 IFL (Integrated Facility for Linux) processors. An IFL is a processor dedicated to and optimized for Linux workloads. Because of SMT, the IFL's appear as 10 logical processors allocated to the partition.

The TOE was tested on an IBM z15 T01 mainframe (machine type 8561)..

The evaluated configuration consists of the specified hardware and software when configured in accordance with the guidance documents listed in the Documentation Section.

7.2 Excluded Functionality

No functionality in the TOE is excluded from the evaluation.

7.3 Operational Environment

The following components must be present in the operational environment to operate the TOE in the evaluated configuration:

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.
Update Server	Yes	Provides the ability to check for updates to the TOE as well as providing signed updates.

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, 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 in accordance with the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for General Purpose Operating Systems, Version 4.2.1 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available and is not duplicated here.

The test tools used in the testing are identified in Section 4 of the Assurance Activity Report [9].

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 the Red Hat Enterprise Linux to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

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 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0].

The validators reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification 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 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0] related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification 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 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0] related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification 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 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and found that the evaluation team provided sufficient evidence and justification 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 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0] , and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for known vulnerabilities on January 15, 2024. All vulnerabilities found were mitigated by vendor patches or by workarounds documented in the User Guidance documents [8]. Users should heed the user guidance. The evaluation team performed vulnerability testing and did not discover any issues with the TOE.

The validators 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0] , 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 [PP_OS_V4.2.1] and Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Administrator Guide document listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need 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 8.6 Security Target, v1.1, January 2024

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 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.
5. Red Hat Enterprise Linux 8.6 Security Target, v1.1, January 2024
6. General Purpose Operating Systems, Version 4.2.1 [PP_OS_V4.2.1]
7. Functional Package for SSH, Version 1.0 [PKG_SSH_V1.0]
8. Red Hat Enterprise Linux 8.6 Common Criteria Guidance, v3.5 January 2024
9. Assurance Activity Report for Red Hat Enterprise Linux 8.6, v 1.1 January 2024
10. Evaluation Technical Report for Red Hat Enterprise Linux 8.6, v1.1 January 2024