National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
for the
Red Hat Enterprise Linux 9.4

Report Number: CCEVS-VR-VID11526-2025

Dated: February 25, 2025

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

Sheldon Durrant

The MITRE Corporation

Farid Ahmed

Robert Wojcik

Anne Gugel

Johns Hopkins University Applied Physics Lab

Common Criteria Testing Laboratory

Kenji Yoshino

Nil Folquer

Nathan Bennett

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Red Hat Enterprise Linux 9.4 provided by Red Hat, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty 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.

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 5-6 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in November 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements of the Protection Profile for General Purpose Operating Systems, Version 4.3 (PP_OS_V4.3), Functional Package for Secure Shell, Version 1.0 (PKG_SSH_V1.0), and Functional Package for Transport Layer Security (TLS), Version 1.1 (PKG_TLS_V1.1).

The TOE is Red Hat Enterprise Linux 9.4. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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). Therefore, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Security Target and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Compliant List (PCL).

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 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
Evaluated Product	Red Hat Enterprise Linux 9.4
Sponsor and Developer	Red Hat, Inc. 100 East Davie Street Raleigh NC, 27601
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	Protection Profile for General Purpose Operating Systems, Version 4.3, 27-September-2022 [PP_OS_V4.3] Functional Package for Secure Shell, Version 1.0, 13-May-2021 [PKG_SSH_V1.0] Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01 [PKG_TLS_V1.1]
ST	Red Hat Enterprise Linux 9.4 Security Target, Version 1. 1, January 2025
Evaluation Technical Report	Red Hat Enterprise Linux 9.4 Evaluation Technical Report, Version 1.3, February 2025
Conformance Result	CC Part 2 extended, CC Part 3 extended
Evaluation Personnel	Kenji Yoshino, Nil Folquer, and Nathan Bennett
CCEVS Validators	Sheldon Durrant, Farid Ahmed, Robert Wojcik, and Anne Gugel

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

Red Hat Enterprise Linux 9.4 is an open-source operating system that supports a general-purpose computing environment for multiple users and applications.

3.1. TOE Evaluated Configuration

The expected use cases (as defined by PP_OS_V4.3) for the TOE are:

- Server System. The OS provides a platform for server-side services, either on physical or virtual hardware.
- Cloud System. The OS provides a platform for providing cloud services running on physical or virtual hardware.

Users interact with the TOE locally (console) via serial connection or remotely (SSH) via a CLI.

3.2. Physical Boundary

The TOE is a software TOE and is comprised of the following:

- Red Hat Enterprise Linux 9.4, build cc-config-9.4-1

The TOE is downloaded by users at: https://access.redhat.com/

The physical boundary of the TOE as it pertains to the evaluated and tested configuration is a compute platform identified in Section 3.3.

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- Update Server. The TOE receives updates from an organization’s local repository via TLS.
- SSH Server. The TOE is capable of securely communicating with an SSHv2 server.
- SSH Client. The TOE is capable of securely communicating with an SSHv2 client.
- Compute Platform. The TOE requires a compute platform meeting the following specifications:
    - Intel Xeon Silver x86-64 UEFI platforms (of Cascade Lake microarchitecture)
    - IBM z16 PR/SM (LPAR) platforms
    - Power10 PowerVM (LPAR) platforms

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates and stores security relevant audit events. These logs are stored locally and are protected by restricting access to system administrators only.

4.2. Cryptographic Support

The TOE implements cryptographic operations in support of its security functions. The correctness of the cryptographic algorithms has been validated through CAVP testing.

4.3. User Data Protection

The TOE implements access controls to prevent unauthorized access to files and directories.

4.4. Identification and Authentication

The TOE supports password and public-key authentication. The TOE supports a configurable password and account lockout policy.

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. 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 TOE Summary Specification section of the ST):

- 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 Allow-lists restrict execution to known/trusted applications.

4.7. TOE Access

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

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

Table 2: Assumptions

Identifier	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.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in PP_OS_v4.3, PKG_SSH_v1.0, and PKG_TLS_v1.1 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 in accordance with the evaluation activities specified in PP_OS_V4.3, PKG_SSH_V1.0, and PKG_TLS_V1.1 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the PP_OS_V4.3, PKG_SSH_V1.0, and PKG_TLS_V1.1 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Red Hat Enterprise Linux 9.4 Common Criteria Guide, Version 1.1 January 2025*
- *Red Hat Enterprise Linux 9.4, Configuring Basic System Settings, 2024-09-06*
- *Red Hat Enterprise Linux 9 Security Hardening, 2024-07-12*
- *Red Hat Enterprise Linux 9 Boot Options for RHEL Installer, 2024-06-25*
- *Red Hat Enterprise Linux 9 Interactively Installing RHEL Over the Network, 2024-07-17*
- *Red Hat Enterprise Linux 9 Interactively Installing RHEL from Installation Media, 2024-08-21*
- *Red Hat Enterprise Linux 9 Configuring Firewalls and Packet Filters, 2024-06-25*
- *Red Hat Enterprise Linux 9 Deploying Web Servers and Reverse Proxies, 2024-06-25*
- *Red Hat Enterprise Linux 9 Securing Networks, 2024-09-13*

All documentation delivered with the product is relevant to and within the scope of the TOE.

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Red Hat Enterprise Linux 9.4 Assurance Activity Report*, Version 1.3, February 2025, provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

8.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing from July 2024 until October 2024. Testing of Intel platform was performed in the Lightship Baltimore facility that has been accredited by NVLAP. Testing of the z16 and Power10 platforms was performed remotely as approved by NIAP according to Policy #31. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

8.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and Table 3 below.

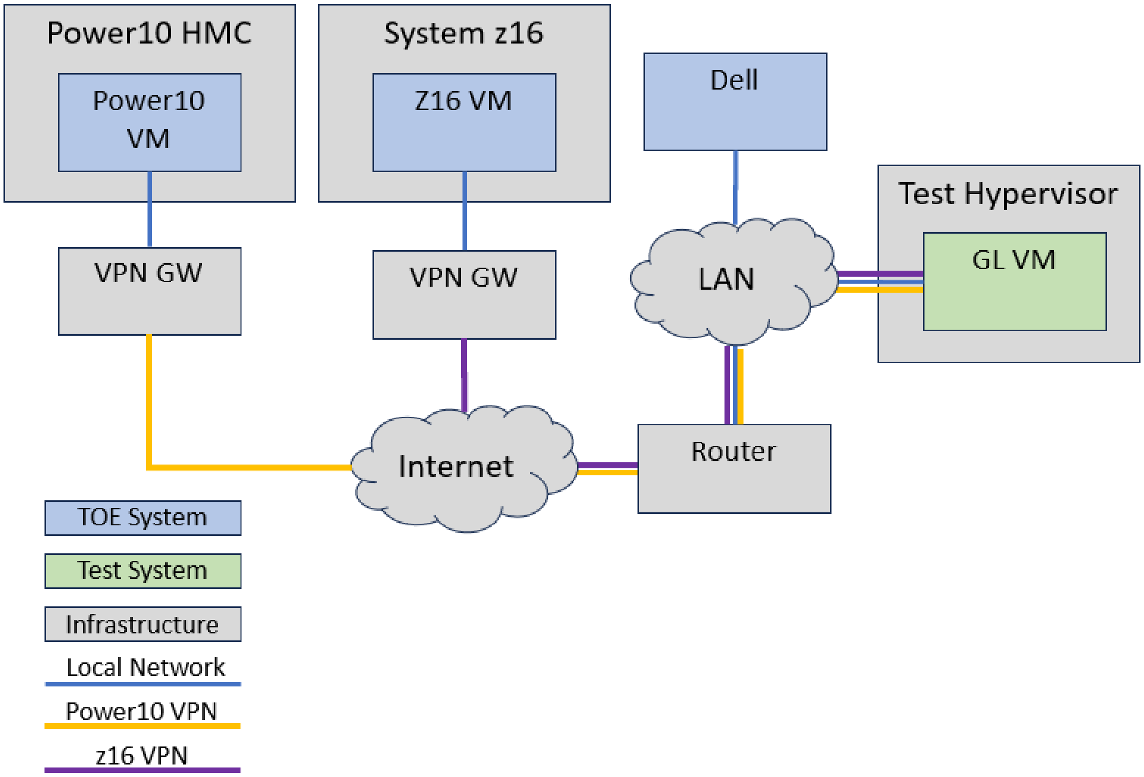

Figure 1: Testing Environment Overview

Table 3 Tools Used for Testing

Tool	Description/Function
gdb 10.2-13	Debugger to control program execution
fmem 1.0.6	Perform memory dumps
bm-search 1.0	Search binary files for binary strings
annocheck 12.31-2	Analyze metadata for executables
dnsmasq 2.89	DNS Server
ntpsec 1.2.3	NTP Server
Greenlight 3.0.35+12719	Lightship test tool suite
Python 3.11.9	Runtime for test tools and scripts
OpenSSL 3.0.1.14	Cryptographic implementation, TLS Client, TLS Server, X.509 Functions
OpenSSH 8.8p1-Lightship-1.1.1	SSH Client, SSH Server
Wireshark 4.2.5	Analyze packet captures
tcpdump 4.99.3	Perform packet captures

Tool	Description/Function
pexpect	Control test execution flow
createrepo-c	Generate update metadata
vsftpd	FTP Server (for installation)
nmap	Perform port scans
Cisco Secure Client 5.0.01242	VPN Client for Z16 environment
Openconnect 9.12-2	VPN Client for Power10 environment
scapy 2.5.0	Perform packet captures

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 all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined Red Hat Enterprise Linux 9.4 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in PP_OS_V4.3, PKG_SSH_V1.0, and PKG_TLS_V1.1.

9.1. Evaluation of Security Target (ASE)

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 9.4 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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 (ADV)

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 ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation team 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.

9.3. Evaluation of Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team 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.

9.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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 (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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.

9.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Red Hat Enterprise Linux 9.4 Vulnerability Assessment*, Version 1.1, February 2025, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on January 27, 2025, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search

The Evaluation team performed a search using the following keywords:

- TOE name
- kernel
- dnf
- audit
- bzip
- chrony
- curl
- fapolicyd

- firewalld
- gpgme
- grub
- gnutls
- gzip
- lz4
- lzo
- openssh
- openssl
- pam
- rpm
- sudo
- tar
- xz
- zlib
- shim
- zipl

The Validation team 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.

9.7. 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 followed the procedures defined in the CEM and performed the Evaluation Activities in PP_OS_V4.3, PKG_SSH_V1.0, and PKG_TLS_V1.1, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11. Annexes

Not applicable.

12. Security Target

Red Hat Enterprise Linux 9.4 Security Target, Version 1.1, January 2025

13. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

14. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

15. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001,* Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002,* Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003,* Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *Protection Profile for General Purpose Operating Systems, Version 4.3, 27-September-2022*
6. *Functional Package for Secure Shell, Version 1.0, 13-May-2021*
7. *Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-03-01*
8. *Red Hat Enterprise Linux 9.4 Security Target, Version 1.1, January 2025*
9. *Red Hat Enterprise Linux 9.4 Common Criteria Guide, Version 1.1 January 2025*
10. *Red Hat Enterprise Linux 9.4, Configuring Basic System Settings, 2024-09-06*
11. *Red Hat Enterprise Linux 9 Security Hardening, 2024-07-12*
12. *Red Hat Enterprise Linux 9 Boot Options for RHEL Installer, 2024-06-25*
13. *Red Hat Enterprise Linux 9 Interactively Installing RHEL Over the Network, 2024-07-17*
14. *Red Hat Enterprise Linux 9 Interactively Installing RHEL from Installation Media, 2024-08-21*
15. *Red Hat Enterprise Linux 9 Configuring Firewalls and Packet Filters, 2024-06-25*
16. *Red Hat Enterprise Linux 9 Deploying Web Servers and Reverse Proxies, 2024-06-25*
17. *Red Hat Enterprise Linux 9 Securing Networks, 2024-09-13*
18. *Red Hat Enterprise Linux 9.4 Evaluation Technical Report, v1.3, February 2025*
19. *Red Hat Enterprise Linux 9.4 Assurance Activity Report, v1.3, February 2025*
20. *Red Hat Enterprise Linux 9.4 Detailed Test Report, v1.2, February 2025*
21. *Red Hat Enterprise Linux 9.4 Dell Test Evidence, v1.1, February 2025*
22. *Red Hat Enterprise Linux 9.4 z16 Test Evidence, v1.1, February 2025*
23. *Red Hat Enterprise Linux 9.4 Power10 Test Evidence, v1.0, December 2024*
24. *Red Hat Enterprise Linux 9.4 Vulnerability Assessment, v1.1, February 2025*