TLP:WHITE

Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Oracle Linux 7.6

19 July 2021

519-EWA

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Oracle Linux 7.6 (hereafter referred to as the Target of Evaluation, or TOE), from **Oracle Corporation** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 19 July 2021 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	**Oracle Linux 7.6**
Developer	**Oracle Corporation**

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

Protection Profile for General Purpose Operating Systems, Version 4.2.1

Extended Package for Secure Shell (SSH), Version 1.0

1.2 TOE DESCRIPTION

The TOE is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

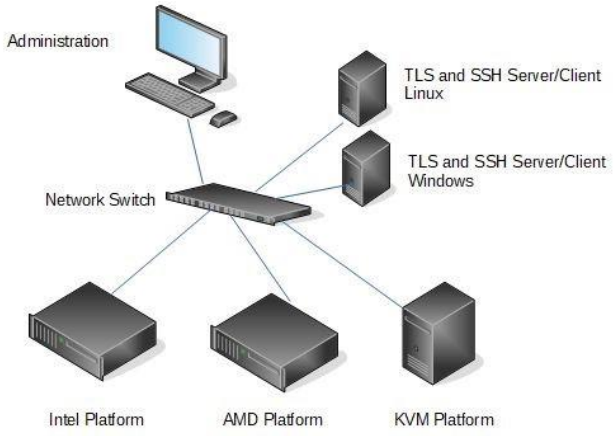

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Audit Data Generation
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CAVP and are used by the TOE:

Table 2: Cryptographic Implementations

Cryptographic Module/Algorithm	Certificate Number
Oracle Linux 7.6 OpenSSL with AESNI, SHA1 AVX, SHA2 ASM	A1400
Oracle Linux 7.6 OpenSSL with AES and SHA1 assembler	A1401
Oracle Linux 7.6 OpenSSL VPAES and SHA1 SSSE3	A1402

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
- 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.
- The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

3.2 CLARIFICATION OF SCOPE

Only the functionality covered by the protection profiles claimed in Section 1.1 is included in the evaluation. The following features/functions are excluded from the evaluation:

- A graphical user interface for system administration or any other operation is not included in the evaluated configuration.
- eCryptFS are not allowed to be used in the evaluated configuration. The encryption capability provided with this file system is therefore unavailable to any user.
- The mandatory access control functionality offered by the Linux Security Module (LSM) framework found in the Linux kernel is not assessed by the evaluation and disabled in the evaluated configuration. All LSM modules such as SELinux, AppArmor, SMACK and others are not assessed as part of the evaluation. The evaluated configuration enables aspects of the LSM though.
- The GSS-API is used to secure the connection between different audit daemons. The security mechanisms used by the GSS-API, however, is not part of the evaluation.
- ECC certificates are not to be used as part of the evaluated configuration.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	Oracle Linux 7.6 + kernel-uek-4.14.35-2025.401.4.el7uek + NetworkManager 1.18.8-1.el7 + NetworkManager-config-server 1.18.8-1.el7 + systemd 219-78.0.1.el7 + sudo 1.8.23-10.el7 + microcode_ctl 2.1-73.0.1.el7 +libpng 1.5.13-8.el7 + grub2 2.02-0.87.0.3.el7 + vim-minimal 7.4.629-7.0.1.el7 + nss 3.35.1-6.0.1.el7_9 + glib2 2.56.1-7.el7 + expat 2.1.0-12.el7 + curl 7.29.0-59.0.1.el7_9.1 + bind-libs-lite 9.11.4-26.P2.el7_9.2 + cpio 2.11-28.el7 + dbus 1.10.24-15.0.1.el7 + e2sfsprogs 1.42.9-19.el7 + freetype 2.8-14.el7_9.1 + libcroco 0.6.12-6.el7_9 + openldap 2.4.44-22.el7 + polkit 0.122-26.0.1.el7 + python 2.7.5-90.0.1.el7 + sqlite 3.7.17-8.el7_7.1 + openssl 1.0.2k-21.el7_9
TOE Hardware	• X86 64-bit Intel Platform with Intel(R) Xeon(R) Silver 4114 processor • EPYC 7551 platform with AMD processor • KVM (kernel based virtual machine) platform

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Oracle Linux 7.6 Common Criteria Guidance Document v1.8, 19 July 2021
b) Oracle Linux 7 Administrator's Guide - E54669-78, October 2020
c) Oracle Linux 7 Installation Guide - E54695-26, October 2020
d) Oracle Linux 7 Security Guide - E54670-27, December 2020

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementation was present in the TOE.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1 PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on **11/18/2020** and included the following search terms:

Oracle Linux 7.6	Oracle Linux CVE	Oracle Linux vulnerabilities
OpenSSL vulnerabilities	Oracle Linux backdoors	Oracle Linux hidden account

Vulnerability searches were conducted using the following sources:

National Vulnerability Database: https://nvd.nist.gov/vuln/search	Oracle support: https://linux.oracle.com/security
Google: http://google.ca	

The independent penetration testing did not uncover any residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Evaluation Technical Report Oracle Linux 7.6, 19 July 2021, v1.4
Security Target Oracle Linux 7.6, 19 July 2021, v4.0
Assurance Activity Report Oracle Linux 7.6, 19 July 2021, v1.3