Swedish Certification Body for IT Security

Certification Report - Oracle Linux 7.3, CSEC2017013

Issue: 1.0, 2019-feb-14

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE,Oracle Linux Version 7 Release 3, is a general purpose, multi-user, multi-tasking Linux based operating system which provides a platform for a variety of applications. In addition, virtual machines provide an execution environment for a large number of different operating systems.

The TOE has been evaluated on the following hardware platforms:

- x86 64-bit Intel Xeon processors:
  - Oracle Server X7-2

The TOE is delivered from the developer, Oracle, using the Oracle delivery mechanism described below. There are several download components: the Oracle Linux 7.3 distribution (ISO) files, and additional packages created specifically for the evaluation of Oracle 7.3 (containing Common Criteria Guide, manual pages for all applications, and configuration files and system calls), and multiple additional packages that must be installed to obtain TOE. The packages and ISO files are delivered via the same delivery mechanism.

Oracle Linux 7.3 is delivered via the Oracle Linux website, an online delivery mechanism provided by Oracle. The integrity and authenticity of the downloadable image files are verified using the SHA-256 hash sums provided on the TLS protected Oracle Cloud download site.

EAL1 augmented by ALC_FLR.3

The Security Target does not claim conformance to any Protection Profile. The TOE meets all functional requirements of the Operating System Protection Profile (OSPP) version 4.1, [OSPPv4.1]

There are three assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the four threats in the ST. The assumptions and the threat are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden and to some extent in the approved foreign location in Munich, Germany and Austin, Texas, USA and was completed on the 30th of January 2019.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 1, augmented by ALC_FLR.3 Flaw reporting procedures.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 1 + ALC_FLR.3.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by atsec information security AB

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2017013
Name and version of the certified IT product	Oracle Linux Version 7 Release 3
Security Target Identification	Security Target for Oracle Linux 7.3, version 1.3, Oracle Corporation, 2019-01-29
EAL	EAL 1 + ALC_FLR.3
Sponsor	Oracle America, Inc.
Developer	Oracle America, Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.22
Recognition Scope	CCRA, SOGIS, EA/MLA
Vulnerability search	2018-12-04
Certification date	2019-02-14

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptographic support
- Identification and authentication
- User data protection
- Protection of the TSF
- TOE access
- Security management
- Trusted Channels / Path

3.1 Auditing

The TOE provides the Lightweight Audit Framework (LAF) which is capable of intercepting all system calls as well as retrieving audit log entries from privileged user space applications. LEF also provides the capability for selecting events to be audited.

3.2 Cryptographic support

The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided. The TOE provides the server side as well as the client side applications. Using OpenSSH, password-based and public-key-based authentication are allowed.

Furthermore, the TOE provides TLS-based communication channels for a cryptographically secured communication with other remote entities. TLS is offered for the key negotiating aspect. The implementations of TLS allow a certificate based authentication of the remote peer (the option for pre-shared keys is disallowed in the evaluated configuration).

Also, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt. Using this device mapper target, the Linux operating system offers administrators and users cryptographically protected block device storage space. With the help of a Password-Based Key-Derivation Function version 2 (PBKDF2) implemented with the LUKS mechanism, a user provided passphrase protects the volume key which is the symmetric key for encrypting and decrypting data stored on disk. Any data stored on the block devices protected by dm_crypt is encrypted and cannot be decrypted unless the volume key for the block device is decrypted with the passphrase processed by PBKDF2. With the device mapper mechanism, the TOE allows for transparent encryption and decryption of data stored on block devices, such as hard disks.

3.3 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.

Using X.509 certificates, users can also perform authentication.

If configured, the password-based authentication utilizes the PAM library.

If the key-based authentication is enabled, the SSH daemon allows the use of RSA or ECDSA keys as authentication token.

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

In addition, the TOE displays informative banners to the users before or during the login to the local console.

3.4 User data protection

The TOE implements Discretionary Access Control (DAC) which allows owners of named objects to control the access permissions to these objects. These owners can permit or deny access for other users based on the configured permission settings. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms.

In addition to the standard Unix-type permission bits for file system objects as well as IPC objects, the TOE implements POSIX access control lists. These ACLs allow the specification of the access to individual file system objects down to the granularity of a single user.

3.5 Protection of the TSF

The TOE protects TSF data via DAC. The TOE provides stack buffer overflow protection with defined compiling option via the GCC compiler. The TOE provides boot integrity via a digital signature with a hardware-protected asymmetric key. Additionally, the TOE can check for and verify digitally signed updates for both the OS itself and application software prior to installation.

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 (ASLR) 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 digital signatures have been successfully validated.

3.6 TOE access

The TOE provides a mechanism to lock a session either automatically after a configurable period of inactivity for that session or upon the user's request.

3.7 Security management

The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to perform the management functions specified in table 6 of [ST].

3.8 Trusted Channels / Path

The TOE protects remote connections with TLS and SSH. The TOE supports TLS v1.2 and SSHv2.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.PROPER_USER - The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.

A.PROPER_ADMIN - The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

4.2 Environmental Assumptions

The Security Target [ST] makes one assumption on the operational environment of the TOE.

A.PLATFORM - The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.

4.3 Clarification of Scope

The Security Target [ST] contains four threats, which have been considered during the evaluation.

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 Architectural Information

The TOE is Oracle Linux which is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications. In addition, virtual machines provide an execution environment for a large number of different operating systems.

The Oracle Linux evaluation covers a potentially distributed network of systems running the evaluated versions and configurations of Oracle Linux as well as other peer systems operating within the same management domain. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSF) consist of functions of Oracle Linux that run in kernel mode plus a set of trusted processes. These are the functions that enforce the security policy as defined in this Security Target. Tools and commands executed in user mode that are used by an administrative user need also to be trusted to manage the system in a secure way. But as with other operating system evaluations they are not considered to be part of this TSF.

The hardware, the BIOS firmware and potentially other firmware layers between the hardware and the TOE are considered to be part of the TOE environment.

The TOE includes standard networking applications, including applications allowing access of the TOE via cryptographically protected communication channels, such as SSH.

System administration tools include the standard command line tools. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a network server using a port above 1024 may be used as a normal application running without root privileges on top of the TOE. The additional documentation specific for the evaluated configuration provides guidance how to set up such applications on the TOE in a secure way.

6 Documentation

Guidance documentation is delivered as part of the ISO distribution. The guidance includes:

- Common Criteria Guide for Oracle Linux 7.3, [CCG]
- Manual pages for all applications, configuration files and system calls

Standard installation process of Oracle Linux is provided in the Oracle Linux Installation Guide for Linux 7 which can be obtained from Oracle website.

7 IT Product Testing

7.1 Developer Testing

Not applicable, in accordance with EAL1.

7.2 Evaluator Testing

The evaluator verified the correct setup test systems according to the documentation in the Evaluated Configuration Guide and the test plan.

The evaluator tested on hardware setup defined in the ST: Oracle Server X7-2. The evaluator executed all of this tests on both two kernel configurations:

- kernel-3.10.0-862.3.3.0.1.el7.x86_64
- kernel-uek-4.1.12-124.16.4.el7uek.x86_64

The evaluator performed all the tests defined in the PP and SSH-EP, which makes it around 100 tests. For the test requirements on crypto primitives and RNG, the tester relied on the CAVS tests that have been performed on the very same system.

Two types of testing was performed: independent testing and algorithm testing on both kernel configurations.

The Independent tests mainly comprised of tests that test the external interfaces, but there were also tests that target TOE security behavior that is normally hidden from the outside:

- key destruction test: this test included the modification of a test client to determine the used keys, with a subsequent search through the TOE physical memory.
- stack protection: a tool has been used that analyses the binary file meta data to determine whether stack protection is enforced
- communication modification: proxy setups where deployed in order to modify live-traffic to exercise the TOE behavior for situations where the TLS protocol is violated

Multiple algorithm testing is required to be performed by [OSPP] and [SSH-EP]. Algorithm Validation System (CAVS) tool version 21.3 was used to generate and validate test vectors for cryptographic algorithms.

7.3 Penetration Testing

The search for vulnerabilities in public vulnerability databases was performed 2018-12-04.

Because the applicable vulnerabilities were either corrected or not exploitable at EAL1, the evaluator only considered the practical verification of the by now widely understood Meltdown vulnerability. Currently, there exist many exploit codes against this issue, which, in the absence of a correct fix, would even allow attackers with a basic attack potential to exploit this weakness.

The penetration test showed that the TOE is not vulnerable for "Meltdown".

Many reported vulnerabilities point out a denial-of-service vulnerability (i.e. TOE crash), and indicate that there might be other impacts, e.g., privilege escalation. However, either no further information is given as to what the how the other impact might be, or how the possible impact could be exploited.

The residual vulnerabilities are: CVE-2017-9150, CVE-2018-14634

8 Evaluated Configuration

The evaluated configurations are defined as follows:

- The CC evaluated package set must be selected at install time in accordance with the description provided in the Evaluated Configuration Guide and installed accordingly.
- The installation specified by the CC guide allows the installation of two different Linux kernels: the Unbreakable Enterprise Kernel (UEK) as well as the derivative of the Red Hat Enterprise Linux kernel. The administrator is free to choose which kernel is used to boot the system as both kernels are allowed in the evaluated configuration.
- The TOE supports the use of IPv4 and IPv6, both are also supported in the evaluated configuration. IPv6 conforms to the following RFCs:
  - RFC 2460 specifying the basic IPv6 protocol<
  - IPv6 source address selection as documented in RFC 3484 Linux implements several new socket options (IPV6_RECVPKTINFO, IPV6_PKTINFO, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_RECVDSTOPTS, IPV6_DSTOPTS, IPV6_RTHDRDSTOPTS, IPV6_RECVRTHDR, IPV6_RTHDR, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_{RECV,}TCLASS) and ancillary data in order to support advanced IPv6 applications including ping, traceroute, routing daemons and others. The following section introduces Internet Protocol Version 6 (IPv6). For additional information about referenced socket options and advanced IPv6 applications, see RFC 3542
  - Transition from IPv4 to IPv6: dual stack, and configured tunneling according to RFC 4213.
- The default configuration for identification and authentication are the defined password-based PAM modules as well as public-key based authentication for OpenSSH. Support for other authentication options, e.g. smart card authentication, is not included in the evaluation configuration.
- If the system console is used, it must be subject to the same physical protection as the TOE.

Deviations from the configurations and settings specified with the Evaluated Configuration Guide are not permitted.

The TOE comprises a single system (and optional peripherals) running the TOE software listed. Cluster configurations are not permitted in the evaluated configuration.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Component*	*Verdict*
Development	ADV	PASS
Functional Specification	ADV_FSP.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.1	PASS
CM Scope	ALC_CMS.1	PASS
Flaw Remediation	ALC_FLR.3	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Objectives	ASE_OBJ.1	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.1	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Independent Testing	ATE_IND.1	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.1	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

AH	Authentication Header
CC	Common Criteria
CEM	Common Methodology for Information Technology Security
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
IKE	Internet Key Exchange
IPSEC	IP Security Protocol
ITSEF	IT Security Evaluation Facility
MAC	Mandatory Access Control
OSPP	Operating System Protection Profile
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE security function
TSFI	TSF Interface
TSP	TOE security policy

12 Bibliography

CC	Common Criteria for Information Technology Security Evaluation, Part 1-3, CCMB-2017-04-001 through 003, version 3.1, revision 5
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, version 3.1, revision 5
ST	Security Target for Oracle Linux 7.3, version 1.3, Oracle Corporation, 2019-01-29
CCG	Common Criteria Guide for Oracle Linux 7.3,Version 1.0, Date 2018-12-20
SSH-EP	Extended Package for Secure Shell, Version 1.0, 2016-02-19
OSPP	Protection Profile for General Purpose Operating Systems, Version 4.1, 2016-03-09 1
SP-002	Evaluation and Certification, CSEC, 2019-01-21, version 30.0
SP-188	Scheme Crypto Policy, CSEC, 2019-01-16, version 8.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.21 valid from 2017-11-15

QMS 1.21.1 valid from 2018-03-09

QMS 1.21.2 valid from 2018-03-09

QMS 1.21.3 valid from 2018-05-24

QMS 1.21.4 valid from 2018-09-13

QMS 1.21.5 valid from 2018-11-19

QMS 1.22 valid from 2019-02-01

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.22". The certifier concluded that, from QMS 1.21.3 to the current QMS 1.22, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability Assessment