Certification Report

Oracle Solaris 11.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-192-CR
Version: 1.0
Date: 18 March 2014
Pagination: i to iii, 1 to 10

DISCLAIMER

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 Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 CCS, 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 the Communications Security Establishment, 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 Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) 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 CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 18 March 2014, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- Oracle is a registered trademark of Oracle Corporation; and
- Solaris is a registered trademark of Oracle Corporation.

TABLE OF CONTENTS

Disclaimer ..... **i**
Foreword ..... **ii**
Executive Summary **1**
1 Identification of Target of Evaluation **2**
2 TOE Description **2**
3 Evaluated Security Functionality **2**
4 Security Target **2**
5 Common Criteria Conformance **3**
6 Security Policy **4**
7 Assumptions and Clarification of Scope **4**
7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 5
7.3 CLARIFICATION OF SCOPE 5
8 Evaluated Configuration **5**
9 Documentation **5**
10 Evaluation Analysis Activities **6**
11 ITS Product Testing **7**
11.1 ASSESSMENT OF DEVELOPER TESTS 7
11.2 INDEPENDENT FUNCTIONAL TESTING 7
11.3 INDEPENDENT PENETRATION TESTING 8
11.4 CONDUCT OF TESTING 8
11.5 TESTING RESULTS 8
12 Results of the Evaluation **9**
13 Evaluator Comments, Observations and Recommendations **9**
14 Acronyms, Abbreviations and Initializations **9**
15 References **10**

Executive Summary

Oracle Solaris 11.1 (hereafter referred to as Solaris 11.1), from Oracle Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Solaris 11.1 is a configurable UNIX-based operating system that securely deploys services in traditional enterprise data centres, large scale cloud environments and small personal desktop use. The operating system includes services such as hardware resource management, and provides services for application software. The operating system is an intermediary between application programs and computer resources. It is responsible for managing processes, processor time, and storage allocation to allow operation of processes and application software.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 24 February 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Solaris 11.1, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security 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 results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Communications Security Establishment, as the CCS Certification Body, declares that the Solaris 11.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Oracle Solaris 11.1 (hereafter referred to as Solaris 11.1), from Oracle Corporation.

2 TOE Description

Solaris 11.1 is a configurable UNIX-based operating system that securely deploys services in traditional enterprise data centres, large scale cloud environments and small personal desktop use. The operating system includes services such as hardware resource management, and provides services for application software. The operating system is an intermediary between application programs and computer resources. It is responsible for managing processes, processor time, and storage allocation to allow operation of processes and application software.

A detailed description of the Solaris 11.1 architecture is found in Section 1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Solaris 11.1 is identified in Section 1 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
OpenSSL FIPS Object Module (Software Version: 1.2, 1.2.1, 1.2.2, 1.2.3 or 1.2.4)	*#1051*
Oracle Solaris Kernel Cryptographic Framework (Software Versions: 1.0 and 1.1)	*#2061*
Oracle Solaris Userland Cryptographic Framework (Software Versions: 1.0 and 1.1)	*#2077*

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Oracle Corporation Solaris 11.1 SRU5.5 Security Target
Version: v1.8
Date: 28 February 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Solaris 11.1 is:

a. Conformant to the BSI Operating System Protection Profile v2.0, 2010-06-01 with the following extended packages;
    - Advanced Management v2.0, 2010-05-28;
    - Extended Identification and Authentication v2.0, 2010-05-28;
    - Labeled Security v2.0, 2010-05-28; and
    - Virtualization v2.0, 2010-05-28.

b. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FCS_RNG.1 Random number generation;
    - FDP_RIP.3 Full residual information protection of resources;
    - FIA_UAU.8 Authentication policy decisions;
    - FIA_UID.3 Identification policy decisions; and
    - FIA_USB.2 Enhanced user-subject binding.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

d. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation

6 Security Policy

Solaris 11.1 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, Solaris 11.1 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Solaris 11.1 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- All connections to and from remote trusted IT systems and between physically separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.
- Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.
- The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
- All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.
- All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.
- Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

7.3 Clarification of Scope

Solaris 11.1 incorporates CAVP-validated cryptography and was subjected to CMVP (FIPS-140) validation. Please refer to the CMVP certificates listed in Section 3 for further details.

8 Evaluated Configuration

The evaluated configuration for Solaris 11.1 comprises:

The TOE software running in a client/server configuration on a GPC with the following requirements;

Category	Requirement
Processors	Either x86 (64-bit), or SPARC architectures.
Memory	The minimum memory requirement is 512 MB.
Disk Space	The recommended size is at least 10 GB. A minimum of 4 GB is required.

The publication entitled *Oracle Solaris 11.1 Guidance Supplement v0.5, February 2014* describes the procedures necessary to install and operate Solaris 11.1 in its evaluated configuration.

9 Documentation

The Oracle Corporation documents provided to the consumer are as follows:

a. Oracle Solaris 11 Security Guidelines, Part No: E29014–02, February 2013;

b. Oracle Solaris Administration: Security Services, Part No: E29015–03, February 2013;

c. Oracle Solaris 11.1 Desktop Administrator's Guide, Part No: E28056-02, February 2013;

d. Solaris 11 XScreenSaver Manual, 28-Sep-2011;

e. Trusted Extensions Configuration and Administration, Part No: E29017–01, October 2012;

f. Trusted Extensions User Guide, Part No: E29018-01, October 2012;

g. Oracle Solaris 11.1 Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, Resource Management, Part No: E29024-01;

h. Securing the Network in Oracle Solaris 11.1, Part No: E28990-02, February 2013;

i. Working With Naming and Directory Services in Oracle® Solaris 11.1, Part No: E29002-01;

j. Installing Oracle Solaris 11.1 Systems, Part No: E28980–01, October 2012;

k. Creating and Administering Oracle Solaris 11.1 Boot Environments, Part No: E29052–01, October 2012; and

l. Adding and Updating Oracle Solaris 11.1 Software Packages, Part No: E28984–02 February 2013.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Solaris 11.1, including the following areas:

Development: The evaluators analyzed the Solaris 11.1 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Solaris 11.1 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Solaris 11.1 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.

Life-cycle support: An analysis of the Solaris 11.1 configuration management system and associated documentation was performed. The evaluators found that the Solaris 11.1 configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Solaris 11.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Solaris 11.1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

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

11.1 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 ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Secure Communication: The objective of this test goal is ensure secure channels for SSH, IPSec (to an LDAP server in the environment) and Kerberos are appropriately encrypted;

c. Label usage: The objective of this test goal is to confirm that labels of files and zones are enforced; and

d. Access restrictions: The objective of this test goal is to confirm that access restrictions based on zones, files, and classifications function properly.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Determine the set of setuid/setgid programs: The objective of this test goal is to determine the set of setuid/setgid programs and see if there are any exploitable weaknesses;

b. MMap NULL pointers: The objective of this test goal is to determine if the NULL pointer can be mmapped;

c. Secure State: The objective of this test goal is to determine that user cannot use Kerberized services when Kerberos is not available;

d. Malicious GIFS: The objective of this test goal is to determine if the printing of malicious GIFS will affect the CUPS server;

e. KADMIND unavailable: The objective of this test goal is to if users can bypass the Kerberos password requirements if kadmind is unavailable;

f. GNOME labeled file copy bypass: The objective of this test goal is to determine if users can bypass the file copy restrictions using the GNOME clipboard;

g. Address leakage: The objective of this test goal is determine if TOE provides information it shouldn't when attacked using the ping-pong attack described in CVE-2002-2443; and

h. Incorrect password change request: The objective of this test goal is to determine if the TOE is susceptible to the password change vulnerability described in CVE-2011-0285.

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

11.4 Conduct of Testing

Solaris 11.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CGI IT Security Evaluation & Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Solaris 11.1 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

An operating system is a complex Target of Evaluation and Solaris 11.1 is no exception. Consumers of the TOE should be familiar with the excluded functionality as detailed in section 3.2 of the administrative guidance supplement. Specifically, a large number of bundled administrative tools and libraries as well as all third party applications have been excluded from the evaluated configuration. No claims are made against them. End users can choose to use or install additional applications as long as such applications do not reconfigure the TOE to take it out of the evaluated configuration.

The CCEF makes two specific recommendations:

1) Due to the complexity of the TOE consumers should ensure only highly trained, experienced individuals be responsible for configuring and administering the TOE; and

2) Administrators are encouraged to review current security alerts and maintain critical patch releases with Oracle Solaris 11.1 by visiting www.oracle.com.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CUPS	Common Unix Printing System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GIF	Graphics Interchange Format
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Oracle Corporation Solaris 11.1 SRU5.5 Security Target, v1.8, 28 February 2014.

e. Oracle Corporation Solaris 11.1 SRU5.5 Common Criteria EAL4+ Evaluation Evaluation Technical Report v1.0 February 24, 2014.