Certification Report

RedSeal Platform v7.0.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-284-CR
Version: 1.0
Date: 30 July 2014
Pagination: i to iii, 1 to 13

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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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 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 CSC Security Testing/Certification Laboratories.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 30 July 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).

TABLE OF CONTENTS

Executive Summary

RedSeal Platform v7.0.1, from RedSeal Networks, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that RedSeal Platform v7.0.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

RedSeal Platform v7.0.1 is a Network Infrastructure Security Management (NISM) platform that continuously identifies attack risk and policy non-compliance in enterprise security infrastructure.

The TOE collects configuration files and vulnerability scans from the network and performs a set of network access checks against all known ingress points within an organization's network infrastructure. It uses this information to build a topology map. It then compares the configurations and data it receives against a set of "best practices" baselines and defined zone-based access policies, to identify high-risk security violations and policy compliance issues such as weak firewall policies, default passwords, insecure services, known vulnerabilities, and access permitted by the as-built network that violates zone access policies. The TOE uses this information, user-defined values assigned to assets, and the asset exposure to threat sources and potential downstream access to provide risk scoring and annotated maps with potential attack vectors.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 10 July 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 RedSeal Platform v7.0.1, 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.

Communications Security Establishment, as the CCS Certification Body, declares that the RedSeal Platform v7.0.1 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 Identification of Target of Evaluation

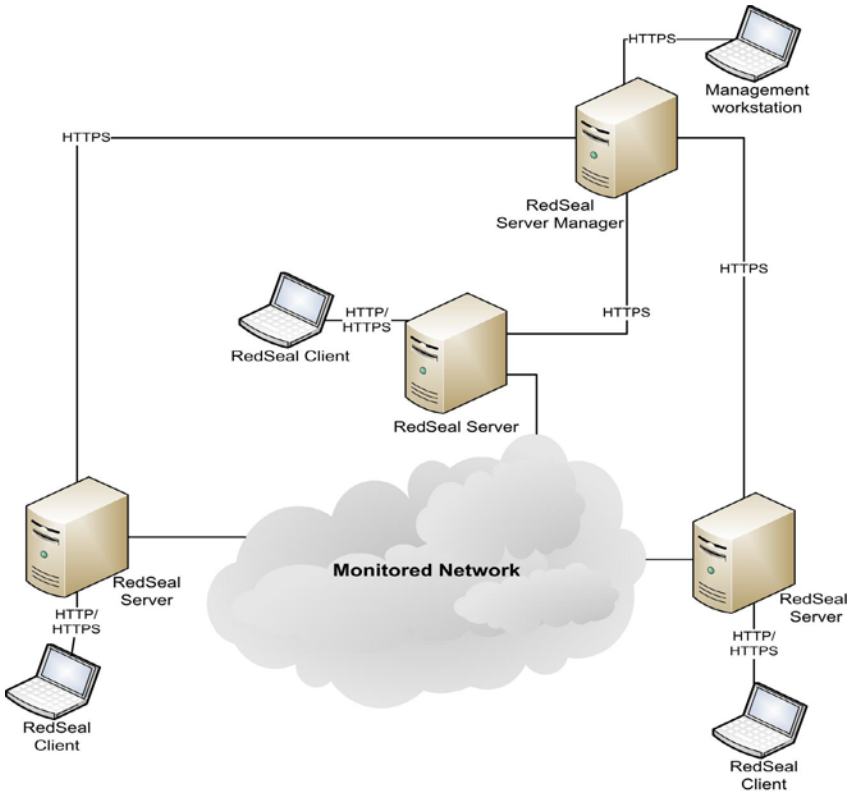
The Target of Evaluation (TOE) for this EAL 2+ evaluation is RedSeal Platform v7.0.1 (hereafter referred to as RedSeal Platform v7.0.1), from RedSeal Networks, Inc.

2 TOE Description

RedSeal Platform v7.0.1 is a Network Infrastructure Security Management (NISM) platform that continuously identifies attack risk and policy non-compliance in enterprise security infrastructure.

The TOE collects configuration files and vulnerability scans from the network and performs a set of network access checks against all known ingress points within an organization's network infrastructure. It uses this information to build a topology map. It then compares the configurations and data it receives against a set of "best practices" baselines and defined zone-based access policies, to identify high-risk security violations and policy compliance issues such as weak firewall policies, default passwords, insecure services, known vulnerabilities, and access permitted by the as-built network that violates zone access policies. The TOE uses this information, user-defined values assigned to assets, and the asset exposure to threat sources and potential downstream access to provide risk scoring and annotated maps with potential attack vectors.

A diagram of the RedSeal Platform v7.0.1 architecture is as follows:



3 Security Policy

RedSeal Platform v7.0.1 implements a role-based access control policy to control administrative access to the system. In addition, RedSeal Platform v7.0.1 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TOE Security Functions*
- *TOE Access*
- *Trusted Path/Channel*
- *Network Assessment*

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

Cryptographic Module	**Certificate**
RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.1 or 6.1.1.0.1)	*#2058*

4 Security Target

The ST associated with this Certification Report is identified below:

RedSeal Networks, Inc. RedSeal Platform v7.0.1 Security Target v1.0, July 9, 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 4.*

RedSeal Platform v7.0.1 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:

- *ALC_FLR.2 – Flaw Reporting procedures*

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:*

- *EXT_FPT_APW.1 - Protection of Administrator Passwords*
- *EXT_NAS_MDC.1 - Monitored Data Collection*
- *EXT_NAS_ANL.1 - Network Analysis*
- *EXT_NAS_RDR.1 - Restricted Data Review*
- *EXT_NAS_STG.1 - Prevention of Monitored Data Loss*

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

6 Assumptions and Clarification of Scope

Consumers of RedSeal Platform v7.0.1 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- Sites deploying the TOE will provide competent, non-hostile TOE administrators and users who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE environment must protect itself and the TOE from external interference or tampering;
- The physical environment must be suitable for supporting a computing device in a secure setting;
- The TOE environment will provide the capability to protect monitored system data as it is transmitted to the TOE;
- The TOE environment must provide reliable timestamps to the TOE; and
- The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

6.3 Clarification of Scope

The following TOE features are not included in the evaluated configuration;

- Admin GUI on Windows platform
- CLI access via SSH

The following was not included within the scope of the evaluation;

- Secure communication between distributed components

7 Evaluated Configuration

The evaluated configuration for RedSeal Platform v7.0.1 comprises:

- RedSeal Client v7.0.1
- RedSeal Server v7.0.1
- RedSeal Server Manager v1.4.0

The Client requires the following;

- Java Standard Edition 7, Update 45;
- Adobe Flash Player 8;
- Internet Explorer v8.0 or Firefox 3.6;
- 100 MB of disk space; and
- 1GB of RAM.

The Server requires the following;

- Windows 7 Enterprise, Windows 8 Enterprise, Windows Server 2003, Windows Server 2008, CentOS v6.2, or Windows Server 2012;
- 300 GB disk space; and
- 8 GB RAM.

When using a virtualized server, the following additional components are required;

- VMware ESX v5.0.

The Server Manager requires the following;

- Windows 7 or Windows Server 2008;
- 2GB disk space and 100 GB of disk for software repository;
- 8 GB RAM; and
- Google Chrome 20 or Firefox Mozilla 10

The publication entitled RedSeal Platform v7.0.1 Guidance Documentation Supplement, v0.5 describes the procedures necessary to install and operate RedSeal Platform v7.0.1 in its evaluated configuration.

8 Documentation

The RedSeal Networks, Inc. documents provided to the consumer are as follows:

a. RedSeal Networks RedSeal Server Manager User Guide, v1.4.0;

b. RedSeal Server Manager Installation Guide, v1.4.0;

c. RedSeal Networks User Guide, v7.0.1;

d. RedSeal Networks Installation and Administration Guide, v7.0.1; and

e. *RedSeal Networks Programmer's Guide and API Reference, v7.0.1.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of RedSeal Platform v7.0.1, including the following areas:

Development: The evaluators analyzed the RedSeal Platform v7.0.1 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 RedSeal Platform v7.0.1 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 RedSeal Platform v7.0.1 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 RedSeal Platform v7.0.1 configuration management system and associated documentation was performed. The evaluators found that the RedSeal Platform v7.0.1 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 RedSeal Platform v7.0.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the RedSeal Platform v7.0.1. 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.

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 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. Resulting from this test coverage approach is the following list of 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. TLS Communication: The objective of this test goal is to confirm the correct functioning of using TLS to protect communication;

c. Checksum Verification: The objective of this test goal is to exercise the integrity mechanism used to verify the TOE;

d. Password Storage: The objective of this test goal is to confirm that passwords are protected from unauthorized access; and

e. Network Assessment: The objective of this test goal is to exercise the network assessment capabilities of the TOE.

[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.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. SQL Injection Exploration: Attempt SQL injection at RedSeal Server Manager web login;

c. RS Manager Priv Escalate: Attempt to escalate privilege by tampering with client side variables;

d. RS Manager Session Attack: Attempt session fixation and prediction attacks;

e. RS Client Local Data: Explore thick client operation and examine local data for credentials;

f. Apache Explore: Attempt to locate default administration pages on Apache web servers; and

g. RMI Metasploit: Attempt exploit of RMI using Metasploit java_rmi_server exploit.

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

10.4 Conduct of Testing

RedSeal Platform v7.0.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evalaution and 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.

10.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that RedSeal Platform v7.0.1 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The evaluators found the RedSeal Platform to be a very useful security intelligence and continuous monitoring tool. The evaluators note that care and attention is required to build the initial network blueprint to extract the most value out of the RedSeal analytical engine. Users should pay particular attention to Chapter 3 'Building a Network Blueprint' of the RedSeal User Guide.

Users should make use of the RedSeal TRL HTTPS plugin configured via the RedSeal Client for automatic TRL updates

13 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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NISM	Network Infrastructure Security Management
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. RedSeal Networks, Inc. RedSeal Platform v7.0.1 Security Target v1.0, July 9, 2014

e. RedSeal Platform v7.0 Evaluation Technical Report v1.0, July 10, 2014.