Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

Riverbed SteelHead CX with RiOS 9.1.4

383-4-376

21 December 2016

v 1.0

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at 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 Common Criteria Scheme – 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 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 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.

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

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

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 Communications Security Establishment.

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 17025:2005, 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 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 Certified Products list (CPL) for the Canadian CC Scheme, and 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

Riverbed SteelHead CX with RiOS 9.1.4(hereafter referred to as the Target of Evaluation, or TOE), from Riverbed Technology, Inc., was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE transparently applies a proprietary algorithm to optimize performance of network traffic and applications across an enterprise network. The TOE optimizes only outbound traffic. The TOE uses TLS to protect optimized user traffic across the WAN. Underlying cryptography is implemented by a Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module.

The TOE provides QoS (Quality of Service), which allows administrators to control the prioritization of different types of network traffic and to ensure that SteelHead CXs give certain network traffic priority over other types of traffic

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 21 December 2016 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 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.

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

1 IDENTIFICATION OF TARGET OF EVALUATION

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

Table 1 TOE Identification

TOE Name and Version	Riverbed SteelHead CX with RiOS 9.1.4
Developer	Riverbed Technology, Inc.
Conformance Claim	EAL 2 + ALC_FLR.1

1.1 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.

1.2 TOE DESCRIPTION

The TOE transparently applies a proprietary algorithm to optimize performance of network traffic and applications across an enterprise network. The TOE optimizes only outbound traffic. The TOE uses TLS to protect optimized user traffic across the WAN. Underlying cryptography is implemented by a Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module.

The TOE provides QoS (Quality of Service), which allows administrators to control the prioritization of different types of network traffic and to ensure that SteelHead CXs give certain network traffic priority over other types of traffic.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

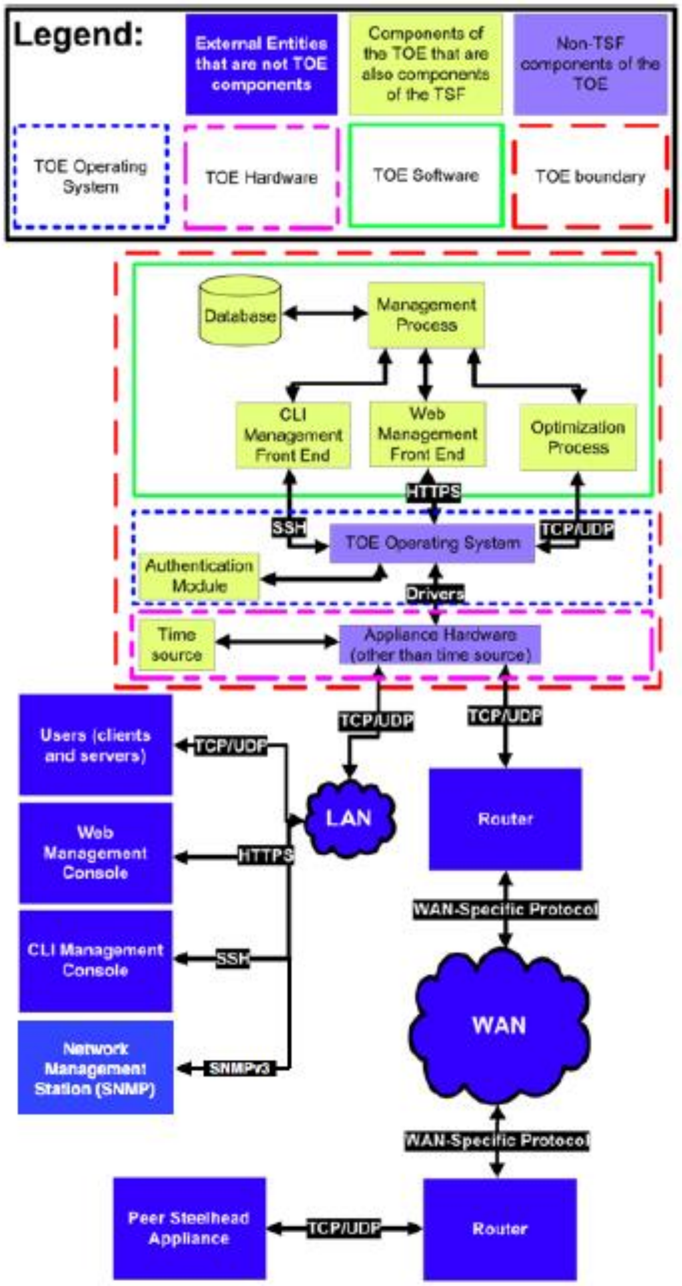

Figure 2: TOE Physical Scope

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit;
- Secure Communications;
- User Data Protection;
- Security Management; and
- Cryptographic Support.

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 module was evaluated by the CMVP and implemented in the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
Riverbed Cryptographic Security Module v1.0	2099

3 ASSUMPTIONS AND CLARIFICATIONS 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 TOE will be installed and configured at an appropriate point in the network according to the appropriate installation guides;
- The TOE environment provides the network connectivity required to allow the TOE to provide secure Wide Area Data Services (WDS);
- The TOE is located within a controlled access facility and is physically available to authorized administrators only;
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance; and
- All ports needed for proper operation of the TOE will be opened at the firewall.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- The hardware and software of the SteelHead CX series, which is made up of the firmware RiOS 9.1.4 on one of the following hardware modules:
  - CX570;
  - CX770;
  - CX3070;
  - CX5070;
  - CX7070/LM; and
  - CX7070H.

4.1 DOCUMENTATION

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

- Network and Storage Card Installation Guide part number 712-00018-21;
- SteelHead Deployment Guide part number 712-00003-21;
- Getting Started Guide part number 712-00102-14;
- SteelHead Installation and Configuration Guide part number 712-00001-21;
- Rack Installation Guide part number 712-00010-21;
- Riverbed Command Line Interface Reference Manual part number 712-00002-23;
- Upgrade and Maintenance Guide part number 712-00016-21;
- SteelHead Management Console User's Guide part number 712-00007-21;
- FIPS Administrator's Guide part number 712-00047-03;
- Riverbed SteelHead CX with RiOS 9.1.4 Operational User Guidance and Preparative Procedures v0.9, 13 December 2016; and
- Riverbed SteelHead CX with RiOS 9.1.4 Monitor Role CLI Reference v1.0, 13 December 2016.

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 TOE 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 TOE 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.

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.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

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 ETR.

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.

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. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Auditing User Login and Logout: The purpose of this testcase is to demonstrate that user`s login or logout via CLI or Web Management consoles are audited;

c. TLS v1.2: The objective of this test goal is to demonstate that the TOE will only support TLS version 1.2 and not connect to a lower version;

d. Inactivity Settings: The objective of this test goal is to demonstrate that inactivity settings work as documented;

e. Management Access Control: The objective of this test goal is to demonstrate that users can only have access to resources based on their assigned permissions;

f. Identification and Authentication: The objective of this test goal is to demonstrate that SNMP command-line access to the TOE requires valid credentials; and

g. SSHv2 Support: The objective of this test goal is to show that the TOE will only use version 2 with the list of supported cryptographic parameters.

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

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:

- Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST;
- Disclosure of exposed Network Services: The objective of this test goal is to scan for open ports using nmap, to ensure disabled services are not seen at accessible interfaces. This information can be used to find potential vulnerabilities in the TOE, and to confirm recommended services have been properly disabled; and
- Password Policy: The objective of this test goal is to verify that proper password management is enforced by the TOE.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any 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 the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

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
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
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 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Riverbed Technology Riverbed Steelhead CX with RIOS 9.1.4 Security Target, version 2, December 2016.
Evaluation Technical Report for Riverbed Technology Riverbed Steelhead CX with RIOS 9.1.4, version 1.1, December 21, 2016.