Certification Report

EAL 3+ Evaluation of Riverbed Cascade Shark v9.6 and Cascade Pilot v9.6

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-206-CR
Version:	1.0
Date:	06 March 2013
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 Canada, 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 Canada, 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 Canada.

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 EWA-Canada.

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 06 March 2013, and the security target identified in Section 0 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 registered trademark:

- Cascade is a registered trademark of Riverbed Technology.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Riverbed Cascade Shark v9.6 and Cascade Pilot v9.6 (hereafter referred to as Cascade Shark v9.6 and Cascade Pilot v9.6), from Riverbed Technology, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Cascade Shark v9.6 and Cascade Pilot v9.6 is a software-only TOE which collects traffic data on a network, calculates performance metrics and alerts the administrators to problems or other conditions.

Cascade Shark facilitates the capture and performance metric calculations of network traffic at high speeds. Cascade Pilot integrates with one or more remote Cascade Shark appliances to provide a centralized analysis and reporting Graphical User Interface (GUI) to administrators of multiple Shark appliances.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 26 February 2013 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 Cascade Shark v9.6 and Cascade Pilot v9.6, 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 3 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.2 – Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Cascade Shark v9.6 and Cascade Pilot v9.6 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) augmented evaluation is Riverbed Cascade Shark v9.6 and Cascade Pilot v9.6 (hereafter referred to as Cascade Shark v9.6 and Cascade Pilot v9.6), from Riverbed Technology.

2 TOE Description

Cascade Shark v9.6 and Cascade Pilot v9.6 is a software-only TOE which collects traffic data on a network, calculates performance metrics and alerts the administrators to problems or other conditions.

Cascade Shark facilitates the capture and performance metric calculations of network traffic at high speeds. Cascade Pilot integrates with one or more remote Cascade Shark appliances to provide a centralized analysis and reporting Graphical User Interface (GUI) to administrators of multiple Shark appliances.

The TOE supports secure communication between distributed TOE components and between the TOE and its remote administrators using FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Cascade Shark v9.6 and Cascade Pilot v9.6 is identified in Section 6 of the ST.

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

Cryptographic Module	**Certificate #**
OpenSSL FIPS Object Module v2.0rc1	1747
Microsoft Windows 7 Kernel Mode Cryptographic Primitives Library (cng.sys)	1328
Microsoft Windows 7 Cryptographic Primitives Library (bcryptprimitives.dll)	1329
Windows XP Enhanced Cryptographic Provider (RSAENH)	989
Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)	990
Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)	997
Windows Vista Enhanced Cryptographic Provider (RSAENH)	893
Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)	894
Microsoft Windows Vista Kernel Mode Security Support	1000

Cryptographic Module	Certificate #
Provider Interface (ksecdd.sys)	
Windows Vista Enhanced Cryptographic Provider (RSAENH)	1002
Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)	1003

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Cascade Shark v9.6 and Cascade Pilot v9.6:

Cryptographic Algorithm	Standard	Certificate #
Advanced Encryption Standard (AES)	FIPS 197	1884, 1168, 1178, 781, 553, 739, 756
Triple-DES (3DES)	FIPS 46-3	846, 675, 676, 677, 549, 656,
Rivest Shamir Adleman (RSA)	ANSI X9.31	559, 560, 731, 255, 258, 353, 354
Secure Hash Algorithm (SHA)	FIPS 180-3	1081, 783, 785, 618, 753
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	677, 428, 429, 412, 407
Random Number Generation (RNG)	ANSI X9.31 Appendix A.2.4	649, 447, 448, 449, 321, 435
Digital Signature Algorithm (DSA)	FIPS 186-3	386, 292, 226, 281

4 Security Target

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

Title: Riverbed Technology Cascade Shark v9.6 and Cascade Pilot v9.6 Security Target
Version: 0.24
Date: 14 January 2013

5 Common Criteria Conformance

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.*

Cascade Shark v9.6 and Cascade Pilot v9.6 is:

a. *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_CKM_EXT.4 - Cryptographic Key Zeroization,

- FCS_TLS_EXT.1 – Extended TLS,
- FCS_HTTPS_EXT.1 – Extended HTTPS,
- FIA_UAU_EXT.5 - Password-based Authentication Mechanism
- FPT_PTD_EXT.1 - Management of TSF Data,
- FPT_TST_EXT.1 – TSF Testing,
- NPM_ANL_EXT.1 - Analysis, and
- NPM_SDC_EXT.1 - System data collection.

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

c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Remediation.

6 Security Policy

Cascade Shark v9.6 and Cascade Pilot v9.6 implements a role-based access control policy to control access to TOE Security Function (TSF) data and administrative functions; details of this security policy can be found in Section 6 of the ST.

In addition, Cascade Shark v9.6 and Cascade Pilot v9.6 implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, protection of the TSF, TOE access, trusted path/channel, and network performance management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Cascade Shark v9.6 and Cascade Pilot v9.6 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 Assumption is listed in the ST:

- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE, and

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

7.3 Clarification of Scope

Cascade Shark v9.6 and Cascade Pilot v9.6 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Cascade Shark and Cascade Pilot v9.6 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Cascade Shark v9.6 and Cascade Pilot v9.6 comprises the following:

- Cascade Shark software v9.6 build number 1004.7291 and the Cascade Shark operating system version 6.1 pre-installed on Cascade Shark hardware;
- Cascade Pilot software v9.6 build number 1004.7291 running on Windows 7 Ultimate Edition, Windows XP Professional and Windows Vista Ultimate Edition;
- FIPS 140-2 validated cryptographic modules included with the Windows operating systems required for the Cascade Pilot; and
- OpenSSL Object Module 2.0 included with the Cascade Shark.

The publication entitled Riverbed Technology Cascade Shark v9.6 and Cascade Pilot v9.6 Guidance Documentation Supplement Version 0.3 describes the procedures necessary to install and operate Cascade Shark v9.6 and Cascade Pilot v9.6 in its evaluated configuration.

9 Documentation

The Riverbed Technology documents provided to the consumer are as follows:

a. Cascade® Shark Installation Guide, Version 9.6 , July 2012;

b. Cascade® Pilot Reference Manual, Version 9.6, July 2012;

c. Cascade® Shark Appliance Quick Start Guide, July 2012;

d. Cascade® Shark Appliance User’s Guide, Version 9.6, July 2012; and

e. Riverbed Technology Cascade Shark v9.6 and Cascade Pilot Guidance Documentation Supplement, Document Version: 0.3, February 15, 2012

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Cascade Shark v9.6 and Cascade Pilot v9.6, including the following areas:

Development: The evaluators analyzed the Cascade Shark v9.6 and Cascade Pilot v9.6 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 Cascade Shark v9.6 and Cascade Pilot v9.6 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Cascade Shark v9.6 and Cascade Pilot v9.6 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 Cascade Shark v9.6 and Cascade Pilot v9.6 configuration management system and associated documentation was performed. The evaluators found that the Cascade Shark v9.6 and Cascade Pilot v9.6 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer’s configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Cascade Shark v9.6 and Cascade Pilot v9.6 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Cascade Shark v9.6 and Cascade Pilot v9.6 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Riverbed Technology for Cascade Shark v9.6 and Cascade Pilot v9.6. During a site visit, the evaluators 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Cascade Shark v9.6 and Cascade Pilot v9.6. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to Cascade Shark v9.6 and Cascade Pilot v9.6 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 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 and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design 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 EWA-Canada test goals:

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

[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.

b. CLI Access: The objective of this test case is to confirm that the operator must authenticate before performing any action on the CLI;

c. Web Access: The objective of this test case is to confirm that the modification of communicated data over the HTTPS web interface will result in an error;

d. Pilot User Interface: The objective of this test case is to confirm that the modification of communicated data over the Pilot user interface will result in an error;

e. Replay Attack: The objective to this test case is to confirm that the Cascade Shark does not respond to replay attacks.

f. TLS Cipher Suites: The objective of this test case is to confirm that the Cascade Shark implements only the TLS cipher suites as described in the ST; and

g. Concurrent Logins: The objective of this test case is to confirm that the Cascade Shark does not allow privilege escalation upon concurrent logins.

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. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to reveal any potential avenues of attack;

b. Vulnerability Identification: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools; and

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer.

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

11.4 Conduct of Testing

Cascade Shark v9.6 and Cascade Pilot v9.6 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 EWA-Canada. 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, giving assurance that Cascade Shark v9.6 and Cascade Pilot v9.6 behaves as specified in its ST and functional specification and TOE design.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products List
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
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
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

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 3, July 2009.

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

d. Riverbed Technology Cascade Shark v9.6 and Cascade Pilot v9.6 Security Target, version 0.24, 14 January 2013.

e. Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of Riverbed Technology Riverbed Cascade Shark v9.6 and Cascade Pilot v9.6 Document No. 1727-000-D002, version 1.0, 26 February 2013.