Certification Report

EAL 4+ Evaluation of BAE Systems STOP OS™ v7.3.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-176-CR
Version: 1.0
Date: 20 January 2012
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 located in Ottawa, 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 20 January 2012, 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 and registered trademarks:

- STOP OS is a trademark of BAE Systems;
- Linux is a registered trademark of Linus Torvalds; and
- Intel is a registered trademark of Intel Corporation.

TABLE OF CONTENTS

Executive Summary

BAE Systems STOP OS™ v7.3.1 (hereafter referred to as STOP v7.3.1), from BAE Systems, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

STOP v7.3.1 is a 32-bit, multiprogramming, multi-tasking, operating system that can support multiple users. In addition to proprietary interfaces for secure administration, STOP v7.3.1 provides a Linux-like user environment and application programming interface (API) that allows Linux and cross-platform applications to be run without change, while benefiting from the designed-in security that STOP v7.3.1 provides.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 13 December 2011 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 STOP v7.3.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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 Canada, as the CCS Certification Body, declares that the STOP v7.3.1 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 BAE Systems STOP OS™ v7.3.1 (hereafter referred to as STOP v7.3.1), from BAE Systems.

2 TOE Description

STOP v7.3.1 is a 32-bit, multiprogramming, multi-tasking, operating system that can support multiple users. In addition to proprietary interfaces for secure administration, STOP v7.3.1 provides a Linux-like user environment and programming interface (API) that allows Linux and cross-platform applications to be run without change, while benefiting from the designed-in security that STOP v7.3.1 provides. The TOE is software-only; the hardware on which STOP v7.3.1 runs is defined to be in the IT environment.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for STOP v7.3.1 is identified in Section 6 of the ST.

The TOE incorporates two FIPS 140-2 validated cryptographic modules that provide cryptographic services to applications.

The first cryptographic modules (CMVP Certificate #1051) implements the following Government of Canada approved cryptographic algorithms:

Cryptographic Algorithm	**Standard**	**Certificate #**
AES	ECB, CBC, and CFB	#695
rDSA	FIPS 186-3	#264
SHA-256, SHA-384, SHA-512	N/A	#723
RNG	N/A	#407

The second cryptographic module (CMVP Certificate #1590) implements the following Government of Canada approved cryptographic algorithms:

Cryptographic Algorithm	**Standard**	**Certificate #**
AES	ECB and CBC	#1603

DRBG	AES_CTR DRBG	#78
HMAC	SHA-256	#939
SHS	SHA-1, SHA-256, SHA-384, and SHA-512	#1416
TRIPLE DES	ECB and CBC	#1048

STOP v7.3.1 implements OpenSSH Version 2 to establish a secure channel to allow remote access to the TOE and uses the following algorithms:

Cryptographic Algorithm	**Standard**	**Certificate #**
AES	FIPS 197	#695
rDSA	FIPS 186	#264

4 Security Target

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

Title: BAE Systems STOP OS™ Version 7.3.1 Security Target
Version: 1.08
Date: December 9, 2011

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.*

STOP v7.3.1 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_BCM_EXT.1 - Baseline Cryptographic Module;
   - FCS_COA_EXT.1 - Cryptographic Operations Availability;
   - FCS_RBG_EXT.1 - Random Number Generation;
   - FIA_AFL_EXT.1 - Authentication Failure Handling; and

- FPT_TST_EXT.1 - TSF testing.

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

c. *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 Policies

STOP v7.3.1 implements six security policies:

- The Cryptographic Module Security Policy is a precise specification of the security rules under which a cryptographic module must operate;
- The Discretionary Access Control policy is a means of restricting access to objects based on the identity of the subjects and the groups to which they belong;
- The Mandatory Access Control Policy is based upon a sensitivity level and sensitivity categories of the subject and sensitivity of the object;
- The Role-based Access Control Policy is used internally by the TSF to prevent modification or deletion of TSF data, including the audit trail and the configuration parameters;
- The Mandatory Integrity Control Policy is based upon an integrity level and integrity categories of the subject and the integrity and integrity categories of the object; and
- The Host-Based Packet Filter Firewall Policy provides functionality that can be configured by an administrator to control network traffic inbound to the TOE and outbound from the TOE.

In addition, STOP v7.3.1 implements policies pertaining to Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Protection of the TSF, TOE Access, Trusted Path/Channel and Security Management.

Further details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of STOP v7.3.1 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

There are no Secure Usage Assumptions listed in the ST.

7.2 Environmental Assumptions

The following Environmental Assumption is 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

STOP v7.3.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. STOP v7.3.1 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 STOP v7.3.1 comprises STOP v7.3.1 with all selectable packages made available during the install process, installed on a host computer meeting the minimum requirement: x86 CPU(s) with the instruction set and features of an i686 [2] or later.

The publication entitled *STOP OS 7.3.1 Trusted Operating System Manual, Appendix: Common Criteria Evaluation Configuration* includes procedures necessary to install STOP v7.3.1 in its evaluated configuration.

9 Documentation

The BAE Systems document provided to the consumer is the *STOP OS 7.3.1 Trusted Operating System Manual*.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of STOP v7.3.1, including the following areas:

Development: The evaluators analyzed the STOP v7.3.1 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TSF interfaces and the TSF subsystems and modules, and

[2] sixth generation Intel x86 microarchitecture

how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the STOP v7.3.1 security architectural description and determined that the initialization process is secure and 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 STOP v7.3.1 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 STOP v7.3.1 configuration management system and associated documentation was performed. The evaluators found that the STOP v7.3.1 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of STOP v7.3.1 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the STOP v7.3.1 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by BAE Systems for STOP v7.3.1. 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.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of STOP v7.3.1. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the STOP v7.3.1 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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[3].

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, TOE design and security architecture description 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; and

b. Independent Testing: The objective of this test goal is to prove or disprove the security claims made by the vendor through positive and negative oriented functional testing. The following independent test cases were executed:

    i. Default User Cannot Access TSF Resources: This test case demonstrates that a default user does not have access to any TSF resources until access is provided by the administrator following user creation;

    ii. Revocation: This test case demonstrates the TSF user revocation capabilities;

    iii. Time Limited Authorization: This test case demonstrates that the administrator can define time-limited authorizations for users;

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

iv. Maximum Number of Concurrent Sessions: This test case demonstrates that the administrator can define a maximum number of active sessions on a case-by-case basis;

v. Protect Authentication Attributes: This test case demonstrates that the administrator can define time-limited authorizations for users;

vi. Authentication Failures: This test case demonstrates that user accounts will be disabled following a preset number of permitted login failures, and will remain disabled until reset by an administrator;

vii. Export of Data Without Security Attributes: This test case demonstrates data can be exported without security attributes provided that the correct access controls are in place, and that all attempts to do so are audited;

viii. Manual Recovery: This test case demonstrates that the TOE will enter a maintenance mode where a manual mechanism is provided to the administrator to return the TOE to a secure state is provided. The test exercises recovery of a corrupted file system in addition to a recovery of a lost administrator password; and

ix. Audit Log Review: This test case pulls the audit log generated during this most recent sequence of tests and conducts a sampling of the log to confirm that the audit data has been generated and logged per the claims in the ST.

11.3 Independent Penetration Testing

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

During the course of the evaluation, it was determined that the TOE security functionality is provided by the primary components STOP v7.3.1 and four third-party applications that have been incorporated into the TOE: Packet Filter firewall, OpenSSL, OpenSSH, and BusyBox. The interfaces to these components were determined to present the most likely sources of TOE vulnerabilities. As a result, the evaluator focused efforts on locating and attempting to exercise potential exploits against these interfaces. Resulting from this analysis approach is the following list of EWA-Canada test goals:

a. Port Scan: The purpose of this test case is to identify all open ports on the TOE;

b. Monitor for Information Leakage: The purpose of this test is to see if the TOE is leaking any information that might be useful to an attacker;

c. Concurrent Admin Sessions: The purpose of this test is to see how the TOE responds to concurrent administrator logins; and

d. SQL Injections: The purpose of this test is to see if the TOE prevents SQL injection attacks at login.

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

11.4 Conduct of Testing

STOP v7.3.1 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 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 STOP v7.3.1 behaves as specified in its ST, functional specification, TOE design and security architecture description.

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

STOP v7.3.1 is a multi-level secure operating system that provides fine grained integrity and sensitivity protection mechanisms. STOP v7.3.1 documentation includes a comprehensive System Manual.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program

Acronym/Abbreviation/ Initialization	Description
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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. BAE Systems STOP OS™ Version 7.3.1 Security Target, Version 1.08, December 9, 2011.

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of BAE Systems STOP OS Version 7.3.1, Version 1.1, 13 December 2011.