Certification Report

HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (running firmware version 3.71), Virtual Connect (running firmware version 4.01), and HP Integrated Lights-Out 3 (version 1.50)

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-209-CR
Version: 1.1
Date: 09 December 2013
Pagination: i to iii, 1 to 12

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 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 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 09 December 2013, 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

HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (running firmware version 3.71), Virtual Connect (running firmware version 4.01), and HP Integrated Lights-Out 3 (version 1.50) (hereafter referred to as HP BladeSystem), from Hewlett-Packard Development Company, L.P., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

HP BladeSystem implements the BladeSystem c-Class architecture, and is optimized for enterprise data center applications (c7000) and midmarket applications (c3000). The enclosures fit into standard 19 inch racks; accommodates BladeSystem c-Class server blades, storage blades, and interconnect modules; and provides all the power, cooling, and I/O infrastructure needed to support them. The Onboard Administrator, Virtual Connect, and iLO components provide the majority of BladeSystem functionality.

The Onboard Administrator is a Linux-based appliance that performs four management functions for the entire enclosure:

- Detecting component insertion and removal
- Identifying components and required connectivity
- Managing power and cooling
- Controlling components

Virtual Connect technology is a set of interconnect modules and embedded software for c-Class enclosures that simplifies the setup and administration of server connections.

The Integrated Lights-Out (iLO) management built into BladeSystem blade servers and storage blades is an autonomous management subsystem embedded directly on the server. iLO monitors each server's overall status, reports issues, and provides a means for setup and managing of power and thermal settings.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 21 October 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 HP BladeSystem, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the HP BladeSystem 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 HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (running firmware version 3.71), Virtual Connect (running firmware version 4.01), and HP Integrated Lights-Out 3 (version 1.50) (hereafter referred to as HP BladeSystem), from Hewlett-Packard Development Company, L.P.

2 TOE Description

HP BladeSystem implements the BladeSystem c-Class architecture, and is optimized for enterprise data center applications (c7000) and midmarket applications (c3000). The enclosures fit into standard 19 inch racks; accommodates BladeSystem c-Class server blades, storage blades, and interconnect modules; and provides all the power, cooling, and I/O infrastructure needed to support them. The Onboard Administrator, Virtual Connect, and iLO components provide the majority of BladeSystem functionality.

The Onboard Administrator is a Linux-based appliance that performs four management functions for the entire enclosure:

- Detecting component insertion and removal
- Identifying components and required connectivity
- Managing power and cooling
- Controlling components

Virtual Connect technology is a set of interconnect modules and embedded software for c-Class enclosures that simplifies the setup and administration of server connections.

The Integrated Lights-Out (iLO) management built into BladeSystem blade servers and storage blades is an autonomous management subsystem embedded directly on the server. iLO monitors each server's overall status, reports issues, and provides a means for setup and managing of power and thermal settings.

A detailed description of the HP BladeSystem architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for HP BladeSystem is identified in Section 1.6 of the ST.

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

Cryptographic Module	**Certificate #**
HP BladeSystem Onboard Administrator Firmware (Firmware Version: 3.71)	*#2174*
iLO 3 Cryptographic Module (Firmware Version: 1.50)	*#2173*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in HP BladeSystem:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	#1439, #1443, #1444, #1445, #1567(VC)
Advanced Encryption Standard (AES)	FIPS 197	#2289, #2294, #2295, #2296, #2297, #2298, #2600(VC)
Rivest Shamir Adleman (RSA)	FIPS 186-2	#1178, #1183, #1182, #1328(VC)
Secure Hash Algorithm (SHA-1)	FIPS 180-2	#1972, #1973, #1977, #1978, #1979, #2184(VC)
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	#1406, #1410, #1607(VC)
Digital Signature Algorithm (DSA)	FIPS 186-2	#716, #720, #788(VC)
ANSI x9.31 Appendix A.4.2 Pseudo Random Number Generator(PRNG)	ANSI x9.31	#1140

4 Security Target

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

Title: Hewlett-Packard Development Company, L.P. BladeSystem c7000 and c3000 Security Target
Version: 1.16
Date: 9 December 2013

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.*

HP BladeSystem is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
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.2 – Flaw Reporting Procedures.

6 Security Policy

HP BladeSystem 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 7.1 of the ST.

In addition, HP BladeSystem implements other 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 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of HP BladeSystem 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:

- Only FIPS-approved ciphers are used by connecting clients (SSH and HTTPS clients) to access VC interconnect modules.
- There are one or more competent individuals assigned to manage the TOE, its operating environment, and the security of the information it contains. The individuals are non-hostile, appropriately trained, and follow all guidance.
- The TOE software will be protected from unauthorized modification.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located within a controlled access facility. If the optional external authentication mechanisms are used, such as LDAP, those external authentication servers are also located within the same controlled access facility and physically and logically on the same secure network as the TOE.

7.3 Clarification of scope

The Virtual Connect cryptography (VC) is only used for secure communication with the TOE, and as such was only validated against CAVP.

8 Evaluated Configuration

The evaluated configuration for HP BladeSystem comprises:

Blade Enclosure	HP BladeSystem c3000 Enclosure; HP BladeSystem c7000 Enclosure
Virtual Connect	HP Virtual Connect Flex-10 10 Gb Ethernet Module; HP Virtual Connect FlexFabric 10 Gb/24-Port Module; HP Virtual Connect Flex-10/10D Module
iLO14	HP iLO 3 Gromit LP on ProLiant G7 server blades; HP iLO 3 Gromit XE on ProLiant G7 server blades
Onboard Administrator	HP BladeSystem c7000 DDR2 Onboard Administrator with KVM ; HP BladeSystem c3000 Tray with embedded DDR2 Onboard Administrator ; HP BladeSystem c3000 Dual DDR2 Onboard Administrator Module

The publication entitled *HP BladeSystem Guidance Documentation Supplement Version 1.0, October 2013* describes the procedures necessary to install and operate HP BladeSystem in its evaluated configuration.

9 Documentation

The Hewlett-Packard Development Company, L.P. documents provided to the consumer are as follows:

a. Technologies in the HP BladeSystem c7000 Enclosure (Part Number 1108878 – December 2011);

b. HP BladeSystem c-Class Solution Overview, Part Number 413339-006, March 2012 (Sixth Edition);

c. HP Integrated Light-Out (iLO) for HP ProLiant Servers (Overview) Part Number DA-12362, September 2012;

d. HP Proliant iLO 3 Scripting and Command Line Guide, Part Number 616297-005, September 2013 (First Edition);

e. HP Integrated Lights-Out security (Technology Brief, 7th Edition) Part Number 101208TB, December 2012;

f. HP iLO 3 User Guide, Part Number 616301-005, September 2013 (First Edition);

g. HP BladeSystem Onboard Administrator Command Line Interface User Guide, Part Number 695523-003, September 2013 (20th Edition);

h. HP BladeSystem Onboard Administrator User Guide, Part Number 695522-004, September 2013 (19th Edition);

i. HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version v4.01 User Guide, Part Number 911532-002, June 2013 (Second Edition); and

j. HP Virtual Connect for c-Class BladeSystem Version 4.01 User Guide, Part Number 711534-002, June 2013 (Second Edition).

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP BladeSystem, including the following areas:

Development: The evaluators analyzed the HP BladeSystem 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 HP BladeSystem 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 HP BladeSystem 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 HP BladeSystem configuration management system and associated documentation was performed. The evaluators found that the HP BladeSystem 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 HP BladeSystem during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP BladeSystem. 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. Hardware failure/CLI tampering: The objective of this test goal is to confirm that the TOE detects hardware failure or tampering from the CLI;

c. FIPS mode: The objective of this test goal is to verify the correct operation of the TOE when FIPS mode is enabled/disabled;

d. User privilege: The objective of this test goal is confirm correct validation and enforcement of user privileges;

e. Login Delays: The objective of this test goal is to verify that login delays between failed login attempts are enforced; and

f. VC external host connections: The objective of this test goal is to confirm that external hosts can/cannot initiate communication to the blade server.

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

b. Testing whether any useful information might be disclosed to an attack by querying the TOE's network interfaces prior to authentication;

c. Attempting a Denial of Service attack on TOE's web interface; and

d. Attempting to connect to the open SNMP port to see if the TOE can be manipulated to cause a security breach.

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

11.4 Conduct of Testing

HP BladeSystem 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 HP BladeSystem 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

The evaluator performed public search for vulnerabilities during independent penetration testing and found invaluable information from the HP security advisories web site. The evaluator recommends the client to subscribe to automatically receive new HP Security Bulletins from the HP IT Resource Center at http://itrc.hp.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
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
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 4, September 2012.

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

d. Hewlett-Packard Development Company, L.P. BladeSystem c7000 and c3000 Security Target, 1.16, 9 December 2013.

e. EAL4+ Common Criteria Evaluation of HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (running firmware version 3.7), Virtual Connect (running firmware version 4.01), and HP Integrated Lights-Out (version 1.5), v1.0, October 21, 2013.