Certification Report

HP BladeSystem c7000 and c3000 Enclosure with OA v4.40, VC v4.41, and iLO 4 v2.11

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-335-CR
Version: 1.0
Date: 15 December 2015
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, 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 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, 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 15 December 2015, 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 OA v4.40, VC v4.41, and iLO 4 v2.11 (hereafter referred to as HP BladeSystem c7000 and c3000), from Hewlett Packard Enterprise Development LP, is the Target of Evaluation. The results of this evaluation demonstrate that HP BladeSystem c7000 and c3000 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

HP BladeSystem c7000 and c3000 is a hardware-software TOE running in two allowable modes of operation. Virtual Connect (VC) Mode comprises a BladeSystem c7000 or c3000 rack-mountable enclosure, one or more Onboard Administrator (OA) modules, one or more VC modules, one or more server blades that include Integrated Lights Out (iLO) functionality, and one or more power supplies. Non-VC Mode includes all of the configuration parameters of VC Mode except there are no VC modules installed in the appliance. The VC modules are replaced with any of the compatible HP pass-through interconnect module options.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 15 December 2015 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 c7000 and c3000, 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 HP BladeSystem c7000 and c3000 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).

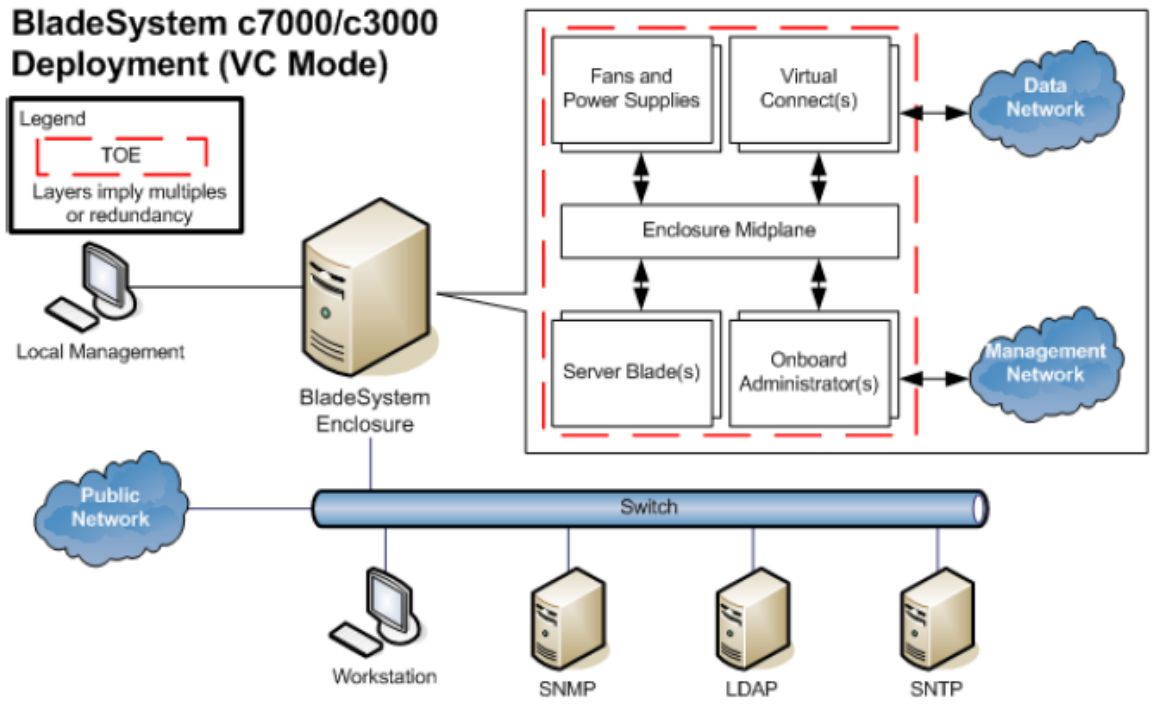
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is HP BladeSystem c7000 and c3000 Enclosure with OA v4.40, VC v4.41, and iLO 4 v2.11 (hereafter referred to as HP BladeSystem c7000 and c3000), from Hewlett Packard Enterprise Development LP.

2 TOE Description

HP BladeSystem c7000 and c3000 is a hardware-software TOE running in two allowable modes of operation. Virtual Connect (VC) Mode comprises a BladeSystem c7000 or c3000 rack-mountable enclosure, one or more Onboard Administrator (OA) modules, one or more VC modules, one or more server blades that include Integrated Lights Out (iLO) functionality, and one or more power supplies. Non-VC Mode includes all of the configuration parameters of VC Mode except there are no VC modules installed in the appliance. The VC modules are replaced with any of the compatible HP pass-through interconnect module options.

A diagram of the HP BladeSystem c7000 and c3000 architecture is as follows:



3 Security Policy

HP BladeSystem c7000 and c3000 implements a role-based access control policy to control administrative access to the system. In addition, HP BladeSystem c7000 and c3000 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

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

Cryptographic Module	**Certificate**
iLO 4 Cryptographic Module	*pending*
HP BladeSystem c-Class Virtual Connect Module	*#2501*
HP BladeSystem Onboard Administrator Firmware	*pending*

4 Security Target

The ST associated with this Certification Report is identified below:

Hewlett-Packard Enterprise Development. LP BladeSystem c7000 and c3000 Security Target, version 2.1, December 15, 2015

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 c7000 and c3000 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 conformant; with security functional requirements based only upon functional components in Part 2;
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 HP BladeSystem c7000 and c3000 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:

- 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

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located within a controlled access facility
- The TOE software will be protected from unauthorized modification

6.3 Clarification of Scope

The following features/functionality were not included within the scope of the evaluation:

- SNMP inbound GET/SET requests
- All iLO SNMP messages
- Remote CLI via Telnet session
- XML44 Reply
- iLO and VC "System Maintenance Switches"
- ProLiant Server Blade operating systems
- Utility Ready Blades (URB)
- Insight Display and KVM (locked in FIPS mode)
- HP Online Configuration Utility (HPONCFG)
- HP Systems Management agent/driver
- Connecting to an IRS device using HP Insight Online
- iLO iOS application
- iLO Android application
- OA running with IPv6 enabled

7 Evaluated Configuration

The evaluated configuration for HP BladeSystem c7000 and c3000 comprises a combination of the following components:

Blade Enclosure

HP BladeSystem c3000 Enclosure

HP BladeSystem c7000 Enclosure

VC (VC Mode Only)

HP VC Flex-10 10Gb Ethernet Module v4.41

HP VC Flex-10/10D Module v4.41

HP VC FlexFabric 10 Gb/24-Port Module v4.41

HP VC FlexFabric-20/40 F8 Module v4.41

Pass-Thru Modules (Non-VC Mode Only)

HP 1Gb Ethernet Pass-Thru Module

HP 4Gb FC Pass-Thru Module

iLO

HP iLO 4 with an Advanced license on ProLiant Gen8 server blades v2.11

HP iLO 4 with an Advanced license on ProLiant Gen9 server blades v2.11

OA

HP BladeSystem c7000 DDR227 Onboard Administrator with KVM28 29 v4.40

HP BladeSystem c3000 Tray with embedded DDR2 Onboard Administrator v4.40

HP BladeSystem c3000 Dual DDR2 Onboard Administrator Module v4.40

Environmental components

LDAP Server (LDAPv3 (RFC32 4511))

SNMP Server (SNMPv3 (RFC 3411 - RFC 3418))

SNTP Server (SNTPv4 (RFC 5905))

The publication entitled Hewlett Packard Enterprise Development LP; BladeSystem c7000 and c3000; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: 1.7 describes the procedures necessary to install and operate HP BladeSystem c7000 and c3000 in its evaluated configuration.

8 Documentation

The Hewlett Packard Enterprise Development LP documents provided to the consumer are as follows:

a. Architecture and Technologies in the HP BladeSystem c3000 Enclosure; HP Part Number: 4AA4-8129ENW; Published: August 2013

b. Architecture and Technologies in the HP BladeSystem c7000 Enclosure; HP Part Number: 4AA4-8125ENW; Published: August 2013

c. HP BladeSystem c3000 Enclosure Quick Setup Instructions; HP Part Number: 446990-005; Published: October 2011; Edition: 5

d. HP BladeSystem c3000 Enclosure Setup and Installation Guide; HP Part Number: 446987-005; Published: February 2013; Edition: 5

e. HP BladeSystem c7000 Enclosure Quick Setup Instructions; HP Part Number: 411762-403; Published: February 2013; Edition: 12

f. HP BladeSystem c7000 Enclosure Setup and Installation Guide; HP Part Number: 411272-401; Published: February 2013; Edition: 10

g. HP BladeSystem c-Class Solution Overview; HP Part Number: 413339-006; Published: March 2012; Edition: 6

h. HP ProLiant Gen8 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 658801-003; Published: November 2013; Edition: 3

i. HP ProLiant Gen9 Troubleshooting Guide Volume II: Error Messages; HP Part Number: 795673-001; Published: September 2014; Edition: 1

j. Pass-Thru Installation Instructions for HP c-Class BladeSystem; HP Part Number: 413280-002; Published: June 2011; Edition: 2

k. HP iLO 4 Release Notes 2.10; HP Part Number 684917-403; Published: March 2015; Edition: 1

l. HP iLO 4 Scripting and Command Line Guide; HP Part Number 684919-009; Published: March 2015; Edition: 1

m. HP iLO 4 User Guide; HP Part Number: 684918-009; Published: March 2015; Edition: 1

n. HP iLO Federation User Guide; HP Part Number: 767159-003; Published: March 2015; Edition: 1

o. HP Integrated Light-Out (iLO) QuickSpecs (Overview); HP Part Number DA-14276; Published: March 2015; Edition: 12

p. Managing HP Servers Using the HP RESTful36 API37 for iLO; HP Part Number 795538-002; Published: March 2015; Edition: 1

q. HP BladeSystem Onboard Administrator 4.40 Release Notes; HP Part Number: 778713-002; Published: March 2015; Edition: 2

r. HP BladeSystem Onboard Administrator Command Line Interface User Guide; HP Part Number: 695523-007; Published: March 2015; Edition: 25

s. HP BladeSystem Onboard Administrator User Guide; HP Part Number: 695522-008; Published: March 2015; Edition: 23

t. HP BladeSystem c-Class Virtual Connect Support Utility Version 1.11.0 User Guide; HP Part Number: 805652-001; Published: February 2015; Edition: 1

u. HP Virtual Connect for c-Class BladeSystem Setup and Installation Guide Version 4.40; HP Part Number: 798321-001; Published: February 2015; Edition: 1

v. HP Virtual Connect 4.40 Release Notes; HP Part Number: 798319-002; Published: March 2015; Edition: 2

w. HP Virtual Connect for c-Class BladeSystem Version 4.40 User Guide; HP Part Number: 798322-001; Published: February 2015; Edition: 1

x. HP Virtual Connect Manager Command Line Interface for c-Class BladeSystem Version 4.40 User Guide; HP Part Number: 798320-001; Published: February 2015; Edition: and

y. Hewlett Packard Enterprise Development LP; BladeSystem c7000 and c3000; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: 1.7

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP BladeSystem c7000 and c3000, including the following areas:

Development: The evaluators analyzed the HP BladeSystem c7000 and c3000 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 c7000 and c3000 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 c7000 and c3000 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 c7000 and c3000 configuration management system and associated documentation was performed. The evaluators found that the HP BladeSystem c7000 and c3000 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 HP BladeSystem c7000 and c3000 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP BladeSystem c7000 and c3000. 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. Failed Login: The objective of this test goal is to confirm that logins to OA subsystem are delayed between failed attempts;

c. Session Timeout: The objective of this test goal is to confirm that a user's session is terminated due to inactivity;

d. SNMP Trap trigger: The objective of this test goal is to confirm that SNMP traps can be sent to the SNMP due to tampering or configuration changes;

e. LDAP Authentication: The objective of this test goal is to confirm that LDAP authentication functions as expected;

f. iLO Federation: The objective of this test goals is demonstrate that one instance of the TOE can control another instance using iLO federation;

g. Pass-thru module: The objective of this test goal is to confirm that the blade servers can communicate to other hosts using the Pass-thru module;

h. Information Flow Control: The objective of this test goal is to confirm that the VC can control the information flow between an external host and the blade server; and

i. UEFI/RBSU access: The objective of this test goal is to confirm that the authentication is required for the iLO UEFI/RBSU interface.

[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; and

b. Big 5 scan: The objective of this test goal is to scan for the current "Big 5" vulnerabilities (Heartbleed, Shellshock, POODLE, GHOST, and FREAK).

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

10.4 Conduct of Testing

HP BladeSystem c7000 and c3000 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that HP BladeSystem c7000 and c3000 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a 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 evaluator recommends the customer to subscribe to HP Security Bulletins notification in order to minimize exploitability of the TOE due to new vulnerabilities.

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
iLO	Integrated Lights Out
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OA	Onboard Administrator
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VC	Virtual Connect

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. Hewlett-Packard Enterprise Development. LP BladeSystem c7000 and c3000 Security Target, version 2.1, December 15, 2015

e. Evaluation Technical Report EAL 2+ Common Criteria Evaluation of HP BladeSystem c7000 and c3000 Enclosure with Onboard Administrator (version 4.40), Virtual Connect (version 4.40), and HP Integrated Lights-Out 4 (version 2.11), v1.0, December 15, 2015.