Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

HPE Integrated Lights-Out 5 v1.11

12 February 2018

383-4-427

Version 1.0

Canada

FOREWORD

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

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

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

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

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

HPE Integrated Lights-Out 5 v1.11 (hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise Development LP, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed 12 February 2018 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

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

1 IDENTIFICATION OF TARGET OF EVALUATION

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

Table 1 TOE Identification

TOE Name and Version	HPE Integrated Lights-Out 5 v1.11
Developer	Hewlett Packard Enterprise Development LP
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

HPE Integrated Lights-Out 5 v1.11 is a hardware-firmware TOE used to simplify initial server setup, monitor server health, provide power and thermal optimization, and provide remote server administration. The TOE is integrated into the motherboard of an HPE ProLiant Gen10 DL or XL server. The TOE is a FIPS 140-2-validated cryptographic module which enables secure communication between system administrators and the TOE and between LDAP and Kerberos servers and the TOE.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

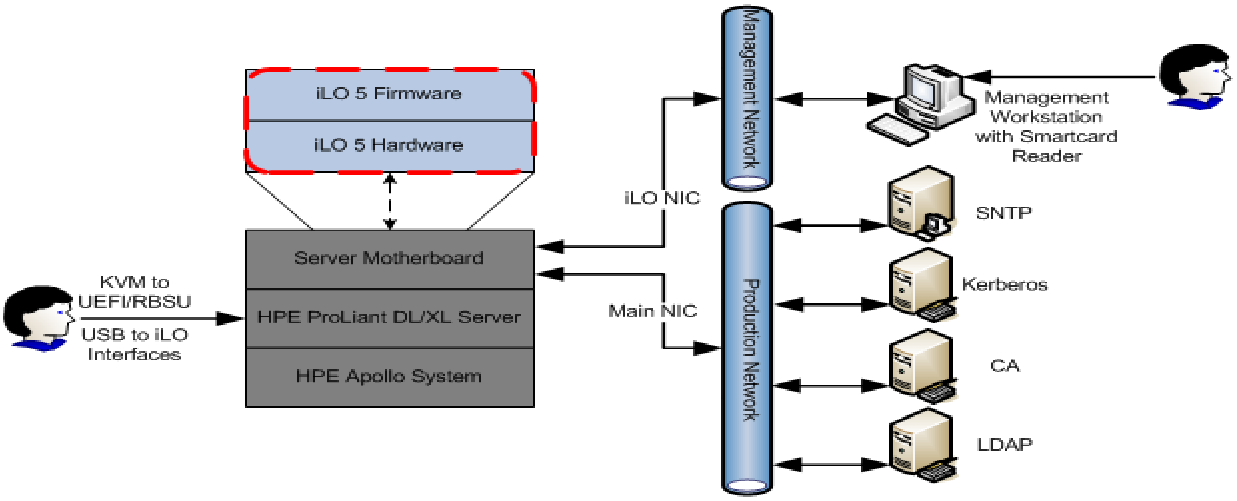

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE 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
- TOE Access
- Trusted Path/Channel

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic module was evaluated by the CMVP and is used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
iLO 5 Cryptographic Module	3122

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

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

3.2 CLARIFICATION OF SCOPE

Features and/or functionality that are not part of the evaluated configuration of the TOE are:

- XML Reply
- iLO System Maintenance Switch
- HPE ProLiant DL/XL server operating systems
- HPE Online Configuration Utility (HPONCFG)
- Connecting to an HPE Insight Remote Support device using HPE Insight Online
- iLO iOS application
- iLO Android application
- Using the iLO service port for mass storage
- Use of SNMP functionality

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the HPE Integrated Lights-Out 5 v1.11 firmware on a GXP Application Specific Integrated Circuit with the iLO Advanced Premium Security Edition license contained within the following host servers:

- HPE ProLiant Gen10 DL360 Rack Server
- HPE ProLiant Gen10 DL380 Rack Server
- HPE ProLiant Gen10 DL560 Rack Server
- HPE ProLiant Gen10 XL230K Scalable Server

The following components are required in the operational environment:

- LDAP Server
- Certificate Authority Server
- SNTP Server
- Kerberos Server
- Smart card reader
- Java Runtime Environment
- Microsoft .NET Framework
- Microsoft, Mozilla Firefox or Google Chrome web browser.

4.1 DOCUMENTATION

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

a. HPE iLO 5 Scripting and Command Line Guide; Part Number 882043-001; Published: July 2017; Edition: 1

b. HPE iLO 5 User Guide; Part Number 880740-001; Published: July 2017; Edition: 1

c. HPE iLO Federation User Guide for iLO 5; Part Number 880724-001; Published: July 2017; Edition: 1

d. UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy; Part Number 881334-001a; Published: July 2017; Edition: 2

e. Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy; Part Number: 873901-002; Published: July 2017; Edition: 1

f. iLO RESTful API Document; https://hewlettpackard.github.io/ilo-rest-api-docs/ilo5/

g. HPE iLO 5 Cryptographic Module; FIPS 140-2 Non-Proprietary Security Policy; FIPS Security Level: 1; Document Version: 0.6

h. Hewlett Packard Enterprise Development LP; Integrated Lights-Out 5 v1.11; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+; Document Version: 0.5

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

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

b. Banner and Authentication Delay: The objective of this test goal is to confirm that the TOE presents an access banner, Kerberos authentication is enforced and a login delay is enforced between failed login attempts on TOE interfaces;

c. Audit Trail Protection: The objective of this test goal is to confirm that access to the audit log is limited to administrators with the appropriate privileges, the audit log is protected from unauthorized modification and deletion and audit logs contain time stamps;

d. iLO CLI Identification and Authentication: The objective of this test goal is to confirm that local and Kerberos authentication methods are enforced for the CLI, password length rules are enforced and only administrators with proper privileges can create new user accounts;

e. iLO Unified Extensible Firmware Interface (UEFI)/ ROM-Based Setup Utility (RBSU) Interface: The objective of this test goal is to confirm that local, Kerberos and LDAP authentication mechanisms are enforced on the iLO UEFI/RBSU interfaces and that restrictions are enforced for the creation of new user accounts;

f. TOE Connections: The objective of this test goal is confirm that communications with the iLO web GUI and the LDAP sever are encrypted and secured using TLS;

g. Personal Identity Verification (PIV) Authentication and Authorization: The objective of this test goal is to demonstrate successful and unsuccessful authentication using PIV cards. This test case will also confirm that appropriate privileges are enforced by the TOE for the authenticated user;

h. iLO USB Service Port: The objective of this test goal is to confirm that the TOE will reject the usage of a USB storage flash drive; and

i. Keyboard Controller Style Interface: The objective of this test is to confirm that the TOE can appropriately process allowed and blocked commands to the TOE from the host OS.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4 INDEPENDENT PENETRATION TESTING

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

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. SNMP Queries: The objective of this test is to attempt to get the TOE to respond to SNMP queries.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

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

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

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
iLO	Integrated Lights-Out
IT	Information Technology
ITS	Information Technology Security
PIV	Personal Identity Verification
PP	Protection Profile
RBSU	ROM-Based Setup Utility
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UEFI	Unified Extensible Firmware Interface

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Hewlett Packard Enterprise Development LP Integrated Lights-Out 5 v1.11 Security Target, Version 0.9, February 12, 2018.
Evaluation Technical Report for the HPE Integrated Lights-Out 5 v1.11 on the GXP Application Specific Integrated Circuit (ASIC) with an Advanced Premium Security Edition license. Version 0.6, February 12, 2018.