Certification Report

HP Universal CMDB and Universal Discovery v10.21

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-336-CR
Version: 1.0
Date: 14 March 2016
Pagination: i to iii, 1 to 11

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 14 March 2016, 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 Universal CMDB and Universal Discovery v10.21, from Hewlett Packard Enterprise Development LP, is the Target of Evaluation. The results of this evaluation demonstrate that HP Universal CMDB and Universal Discovery v10.21 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

HP Universal CMDB and Universal Discovery v10.21 is a federated CMS (Configuration Management System) that discovers and collects data from physical and logical entities and services in the IT network. To discover the physical and logical network entities, the TOE uses Discovery Activities. Each Discovery Activity contains a discovery schedule and the required credentials to access the network entities.

Collected data is stored and analyzed upon reception by the TOE, allowing TOE administrators to perform impact analysis on proposed configuration changes, policy management and enforcement, and change tracking and control. Each physical or logical entities discovered and collected by the TOE is referred to as a CI (Configuration Item). The TOE maintains baseline profiles for CIs, known as CITs (Configuration Item Templates). If a CI is detected to be different than the configuration specified in the CIT, TOE administrators may notify the CI's stakeholders, asking whether a change is required to address the discrepancy. In addition to comparing the CIs with the expected configuration according to a CIT, the TOE is able to compare the CI against TOE administrator configured policies. These policies can be related to the physical resources, configuration, or deployment needs of the CI.

The TOE provides management capabilities through the UCMDB user interface (UI), a JMX interface to the UCMDB server, the exposed SDK API of the UCMDB server, the CM UI, a JMX interface to CM, and a JMX interface to the UD (Universal Discovery)Probe. The management capabilities available over the UCMDB SDK API are identical to the management capabilities available over the UCMDB UI.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 14 March 2016 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 Universal CMDB and Universal Discovery v10.21, 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 Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 (hereafter referred to as HP Universal CMDB and Universal Discovery v10.21), from Hewlett Packard Enterprise Development LP.

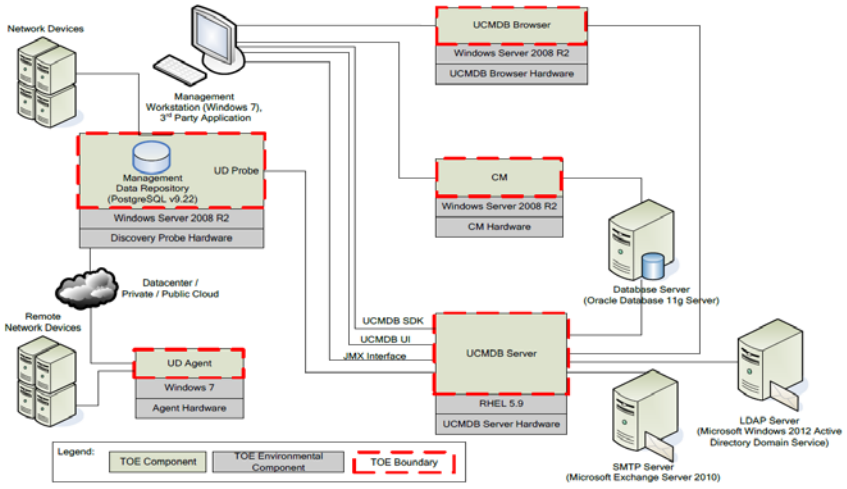
2 TOE Description

HP Universal CMDB and Universal Discovery v10.21 is a federated CMS (Configuration Management System) that discovers and collects data from physical and logical entities and services in the IT network. To discover the physical and logical network entities, the TOE uses Discovery Activities. Each Discovery Activity contains a discovery schedule and the required credentials to access the network entities.

Collected data is stored and analyzed upon reception by the TOE, allowing TOE administrators to perform impact analysis on proposed configuration changes, policy management and enforcement, and change tracking and control. Each physical or logical entities discovered and collected by the TOE is referred to as a CI (Configuration Item). The TOE maintains baseline profiles for CIs, known as CITs (Configuration Item Templates). If a CI is detected to be different than the configuration specified in the CIT, TOE administrators may notify the CI's stakeholders, asking whether a change is required to address the discrepancy. In addition to comparing the CIs with the expected configuration according to a CIT, the TOE is able to compare the CI against TOE administrator configured policies. These policies can be related to the physical resources, configuration, or deployment needs of the CI.

The TOE provides management capabilities through the UCMDB user interface (UI), a JMX interface to the UCMDB server, the exposed SDK API of the UCMDB server, the CM UI, a JMX interface to CM, and a JMX interface to the UD (Universal Discovery)Probe. The management capabilities available over the UCMDB SDK API are identical to the management capabilities available over the UCMDB UI.

A diagram of the HP Universal CMDB and Universal Discovery v10.21 architecture is as follows:



3 Security Policy

HP Universal CMDB and Universal Discovery v10.21 implements a role-based access control policy to control administrative access to the system. In addition, HP Universal CMDB and Universal Discovery v10.21 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/channels
- Universal Discovery and Configuration Management

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

Cryptographic Module	**Certificate**
RSA BSAFE Crypto-J JSAFE and JCE Software Module, Software Version 6.1	*#2057*
OpenSSL FIPS Object Module, Software Version 2.0.7	*#1747*

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Security Target, version 1.1, March 11, 2016

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 Universal CMDB and Universal Discovery v10.21 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 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - EXT_UDC_CID - Configuration Item Discovery
    - EXT_UDC_PCC - Policy Creation and Compliance
    - EXT_UDC_PCA - Policy Compliance Alerting
    - EXT_UDC_RDR - Restricted data review
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 Universal CMDB and Universal Discovery v10.21 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 Assumptions are listed in the ST:

- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and
- Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware and operating system;
- The TOE is located within a controlled access facility;
- The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions;
- The TOE software will be protected from unauthorized modification;
- The TOE environment will provide the TOE with the necessary reliable timestamps; and
- The TOE environment will include a trusted network that is protected from external interference and tampering.

7 Evaluated Configuration

The evaluated configuration for HP Universal CMDB and Universal Discovery v10.21 comprises The TOE components (see section 2) installed on the following;

- GPC server running RHEL v5.9 (UCMDB Server only),
- GPC server running Windows Server 2008 R2 64-bit OS (UCMDB Browser, CM, and UD Probe), and
- GPC running Windows 7 64-bit OS (UD Agent only).

The following environmental components are required;

- Authentication Server to support LDAP
- Oracle 11g Database Server
- Simple Mail Transfer Protocol (SMTP) Server

The publication entitled HP Universal CMDB and Universal Discovery v10.21 Guidance Documentation Supplement v0.7 describes the procedures necessary to install and operate HP Universal CMDB and Universal Discovery v10.21 in its evaluated configuration.

8 Documentation

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

a. HP Universal CMDB, Software Version 10.21, Administration Guide, Document Release Date: July 2015, Software Release Date: July 2015;

b. HP Universal CMDB, Software Version 10.21, Developer Reference Guide, Document Release Date: July 2015, Software Release Date: July 2015;

c. HP Universal CMDB, Software Version 10.21, JMX Reference Guide, Document Release Date: July 2015, Software Release Date: July 2015;

d. HP Universal CMDB and Configuration Manager, Software Version 10.21, Hardening Guide, Document Release Date: July 2015, Software Release Date: July 2015;

e. HP Universal CMDB Configuration Manager, Software Version 10.21, User Guide, Document Release Date: July 2015, Software Release Date: July 2015;

f. HP Universal CMDB, Software Version 10.21, HP UCMDB 10.21 Release Notes, Document Release Date: July 2015, Software Release Date: July 2015; and

g. HP Universal CMDB, Software Version 10.21, Support Matrix, Document Release Date: July 2015, Software Release Date: July 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP Universal CMDB and Universal Discovery v10.21, including the following areas:

Development: The evaluators analyzed the HP Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 configuration management system and associated documentation was performed. The evaluators found that the HP Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP Universal CMDB and Universal Discovery v10.21. 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. Generation of Audit records: The objective of this test goal is to confirm the generation of audit records not tested by the developer;

c. Authentication via LDAP: The objective of this test goal is to confirm that the TOE supports LDAP authentication;

d. Discovery and Review of CI's over SSH: The objective of this test goal is to confirm that the TOE can discover and review configuration items over SSH;

e. Create a policy: The objective of this test goal is to demonstrate that TOE admins can create policies and view the change history of a CI;

f. User Privileges: The objective of this test goal is test user privileges; and

g. SSL comunication: The objective of this is to confirm that the UCMDB server communicates with the CM and UD Probe over TLS.

[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(For example Heartbleed, Freak, Poodle, Ghost, Shellshock)

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

10.4 Conduct of Testing

HP Universal CMDB and Universal Discovery v10.21 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 Universal CMDB and Universal Discovery v10.21 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CI	Configuration Item
CIT	Configuration Item Type
CPL	Certified Products List
CM	Configuration Management
CMDB	Configuration Management Database
CMS	Configuration Management System
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
TSF	TOE Security Function
UD	Universal Discovery

13 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. Security Target: Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Security Target, version 1.1, March 11, 2016

e. Hewlett Packard Enterprise Development LP HP Universal CMDB and Universal Discovery v10.21 Common Criteria EAL2 Evaluation Technical Report v0.4,March 14, 2016 .