COMMON CRITERIA CERTIFICATION REPORT

Hewlett Packard Enterprise StoreOnce System Version 3.13

383-4-364

13 October 2016

v1.0

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. 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 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

Hewlett Packard Enterprise StoreOnce System Version 3.13 (hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise, was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a disk-based storage appliance used for backing up host network servers to target devices on the appliance. These devices are configured as Network-Attached Storage (NAS), Virtual Tape Library (VTL) or StoreOnce Catalyst stores. The TOE includes hardware-based RAID 6 to reduce the risk of user data loss due to disk failure. The TOE is managed in the form of a Graphical User Interface (GUI) or Secure Shell (SSH) protected Command Line Interface.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 13 October 2016 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 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	Hewlett Packard Enterprise StoreOnce System Version 3.13
Developer	Hewlett Packard Enterprise
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

The TOE is a disk-based storage appliance used for backing up host network servers to target devices on the appliance. These devices are configured as Network-Attached Storage (NAS), Virtual Tape Library (VTL) or StoreOnce Catalyst stores. The TOE includes hardware-based RAID 6 to reduce the risk of user data loss due to disk failure. The TOE is managed in the form of a GUI or SSH protected command line interface. Management sessions are protected using Cryptographic Algorithm Validation Program (CAVP) validated cryptography.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

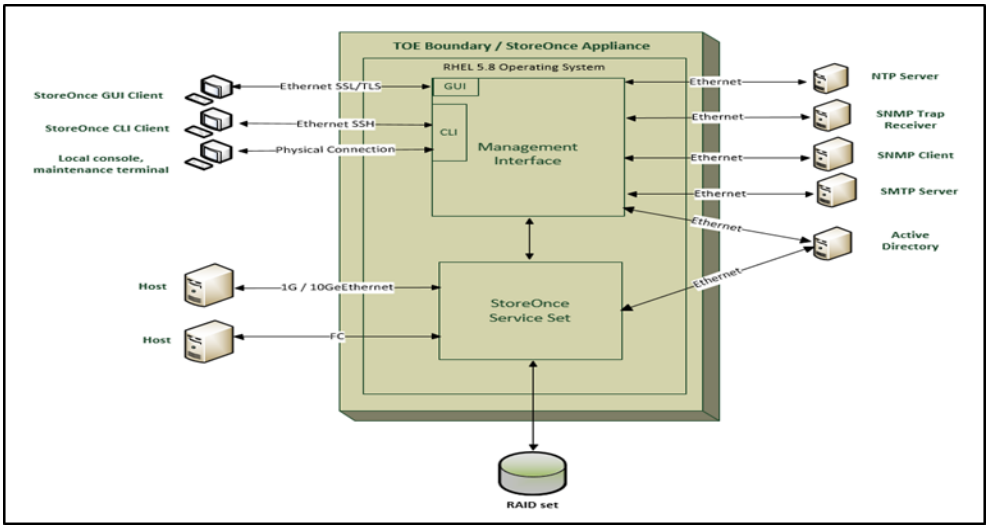

Figure 1 TOE Architecture

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 TOE Security Functionality
- TOE Access
- Trusted Path/Channels

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 Government of Canada approved cryptographic algorithms were evaluated by the Cryptographic Algorithm Validation Program for correct implementation in the TOE:

Table 2 Cryptographic Algorithms

Cryptographic Algorithm	Standard	Certificate Number
Triple-DES (3DES)	FIPS 46-3	2249
Advanced Encryption Standard (AES)	FIPS 197	4119, 3994
Rivest Shamir Adleman (RSA)	FIPS 186-4	2050
Secure Hash Algorithm (SHS)	FIPS 180-3	3388, 3296
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	2690

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:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- Fibre Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary.
- A dedicated and protected management network exists between nodes of the TOE and hosts providing supporting services (e.g. NTP, SNMPv3, SMTP or AD).
- Confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment.
- A dedicated and protected internal network exists that connects nodes of the TOE with network storage devices.
- It is assumed that network devices on the internal network do not intercept, impersonate or otherwise modify communications on the internal network.

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the HPE StoreOnce System, Version 3.13 build 3-1612.1 software running on the StoreOnce 6500 system appliance.

4.1 DOCUMENTATION

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

a. HPE StoreOnce 6500 and B6200 Backup System User Guide, Edition 12, August 2015.

b. HPE StoreOnce System CLI Reference Guide, Edition 11, September 2015.

c. HPE StoreOnce System Linux and UNIX Configuration Guide for G3, Edition 6.0, August 2015.

d. HPE StoreOnce Series Backup system Installation Planning and Preparation Guide and Checklists, Edition 4, August 2015.

e. HPE StoreOnce System Version 3.13 Guidance Supplement, Version 0.3.

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 TOE 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 TOE 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.

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.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. 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 TOE.

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 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.

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. Simple Network Management Protocol (SNMP) Agent and SNMP Traps: The objective of this test case is to demonstrate that Management Information Base objects can be accessed by valid SNMP users and that the TOE can be configured to send SNMP messages to a SNMP trap receiver;

c. Simple Mail Transfer Protocol (SMTP): The objective of this test case is to confirm that the TOE is capable of sending e-mail;

d. Fibre Channel (FC) and VTL: The objective of this test case is to demonstrate that access control is enforced for the FC and the VTL library;

e. Catalyst store: The objective of this test case is to demonstrate that access control is enforced for the Catalyst store;

f. Network File Share (NFS): The objective of this test case is to demonstrate that access control is enforced for NFS shares;

g. Common Internet File System (CIFS): The objective of this test case is to demonstrate that access control is enforced for CIFS shares;

h. Transport Layer Security (TLS): The objective of this test case is to demonstrate that the web GUI is secured with TLS;

i. SSH: The objective of this test case is to demonstrate that the CLI is secured with SSH;

j. CLI: The objective of this test case is to demonstrate the commands available to the administrator via the CLI; and

k. Audit Retention: The objective of the test case is to demonstrate that the TOE retains audit records based on the retention period set by the administrator.

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;

b. Cookie Strength: The objective of this test is to determine whether the TOE is susceptible to weak session IDs;

c. Session Fixation: The objective of this test is to determine whether the TOE is susceptible to session fixation; and

d. Weak Algorithms in SSH and TLS: The objective of this test is to determine whether the TOE offers weak algorithms for SSH and TLS.

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 the 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.

8 EVALUATOR COMMENTS, OBSERVATIONS AND RECOMMENDATIONS

The TOE is a sophisticated storage system therefore the customer is well advised to follow the instructions in the Guidance Supplement, HPE StoreOnce System Version 3.13 and the installation and configuration guidance documentation which is listed in Section 4.1.

9 SUPPORTING CONTENT

9.1 LIST OF ABBREVIATIONS

Term	Definition
AD	Active Directory
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
HPE	Hewlett Packard Enterprise
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SFR	Security Functional Requirement

Term	Definition
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VTL	Virtual Tape Library

9.2 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.
HPE StoreOnce System Version 3.13 Security Target, Version 1.2, October 13, 2016.
Hewlett Packard Enterprise StoreOnce System, Version 3.13 Common Criteria EAL 2+ Evaluation Technical Report, Version 0.5, October 13, 2016.