Certification Report

HP 3PAR StoreServ Storage Systems Version 3.2.1 MU3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-341-CR
Version: 1.0
Date: 07 December 2015
Pagination: i to iii, 1 to 9

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 07 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 3PAR StoreServ Storage Systems Version 3.2.1 MU3 (hereafter referred to as HP 3PAR StoreServ Version 3.2.1 MU3), from Hewlett Packard, is the Target of Evaluation. The results of this evaluation demonstrate that HP 3PAR Version 3.2.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

HP 3PAR StoreServ Version 3.2.1 MU3 are hardware appliances that serve to host physical disk drives and provide a secure channel to configure the access control policy that is enforced between the content on the disk drives and the attached Storage Area Network hosts. Administrators manage the storage systems using the HP 3PAR OS Version 3.2.1 MU3 Command Line Interface client application, which is installed on management computers and provides a secure tunnel from which to access the available security management functions. The TOE also uses a secure tunnel to communicate with an external key manager server.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 07 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 3PAR StoreServ Version 3.2.1 MU3, 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 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Storage Systems Version 3.2.1 MU3 (hereafter referred to as HP 3PAR StoreServ Version 3.2.1 MU3), from Hewlett Packard.

2 TOE Description

HP 3PAR StoreServ Version 3.2.1 MU3 are hardware appliances that serve to host physical disk drives and provide a secure channel to configure the access control policy that is enforced between the content on the disk drives and the attached Storage Area Network hosts. Administrators manage the storage systems using the HP 3PAR OS Version 3.2.1 MU3 Command Line Interface client application, which is installed on management computers and provides a secure tunnel from which to access the available security management functions. The TOE also uses a secure tunnel to communicate with an external key manager server.

3 Security Policy

HP 3PAR StoreServ Version 3.2.1 MU3 implements a role-based access control policy to control administrative access to the system. In addition, HP 3PAR Version 3.2.1 MU3 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*
- *Trusted path/channels*

The following cryptographic module is used to secure TOE communications with an external key manager server and was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
OpenSSL FIPS module v2.0.8	1747

The TOE also provides cryptographic support for communications on the management path. The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in HP 3PAR Version 3.2.1.

Cryptographic Algorithm	**Standard**	**Certificate #**
AES CTR and CBC (128-256 bits)	FIPS PUB 197 NIST SP 800-38A	Cert # 3631 (libcrypto) and Cert #3633 (libgcrypt)
RSA Digital Signature Algorithm (rDSA) (modulus 1024 and 2048)	FIPS PUB 186-2	Cert # 1872 (libcrypto) and Cert # 1874 (libgcrypt)
SHA-1 and SHA-256 (digest sizes 160, 256)	FIPS Pub 180-3	Cert #3049 (libcrypto) and Cert # 3051 (libgcrypt)
HMAC-SHA-1 (digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	Cert # 2382 (libcrypto) and Cert # 2384 (libgcrypt)

4 Security Target

The ST associated with this Certification Report is identified below:

Hewlett-Packard 3PAR StoreServ Storage Systems Security Target, Version 5.0, December 07, 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 3PAR StoreServ Version 3.2.1 MU3 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:
- FDP_AVL_EXT.1 – User Data Availability
- FPT_APW_EXT.1 – Protection of Administrator Passwords
- FPT_TST_EXT.1 – TSF Testing

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 3PAR StoreServ Version 3.2.1 MU3 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:

- *TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Internet Small Computer Systems Interface and Fiber Channel host identities properly reflect the adapters and the hosts to which they are associated.*
- *Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment, which includes the client hosts.*
- *A Network Time Protocol server provides reliable timestamps for use by the TOE.*

7 Evaluated Configuration

The evaluated configuration for HP 3PAR Version 3.2.1 MU3 comprises the following HP 3PAR StoreServ hardware models running the HP 3PAR operating system version 3.2.1 MU3:

- 7200c;
- 7400c;
- 7440c;
- 7450c;
- 10400;
- and 10800[1]

The publication entitled HP 3PAR OS 3.2.1 Common Criteria Administrator's Reference describes the procedures necessary to install and operate HP 3PAR StoreServ Version 3.2.1 MU3 in its evaluated configuration.

8 Documentation

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

[1] The StoreServ 10400 and 10800 models identify themselves as InServ V400 and InServ V800, respectively.

a. HP 3PAR OS 3.2.1 Concepts Guide;

b. HP 3PAR OS 3.2.1 CLI Administrator's Manual;

c. HP 3PAR OS 3.2.1 Command Line Interface Reference; and

d. HP 3PAR OS 3.2.1 Common Criteria Administrator's Reference.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of HP 3PAR Version 3.2.1 MU3, including the following areas:

Development: The evaluators analyzed the HP 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Version 3.2.1 MU3 configuration management system and associated documentation was performed. The evaluators found that the HP 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Version 3.2.1 MU3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the HP 3PAR StoreServ Version 3.2.1 MU3. 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[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.

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. Lightweight Directory Access Protocol (LDAP) authentication and LDAP over TLS/SSL: The objective of this test goal is to verify the TOE's use of LDAP for authentication and to confirm that communication between the TOE and the LDAP server is protected with TLS/SSL;

c. Public Key Authentication: The objective of this test goal is to confirm that the TOE can authenticate users using Public Key Authentication;

d. External Key Manager Server Connection: The objective of this test goal is to confirm that that the external key manager server connection is protected with TLS/SSL;

e. Audit Log: The objective of this test goal is to confirm that the TOE provides capabilities for audit log generation, audit log review, and audit log storage protection; and

f. Verification of Cryptographic Module and Algorithms: The objective of this test goal is to verify the cryptographic module and algorithms incorporated within the TOE.

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:

[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.

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

b. Heartbleed: The objective of this test goal is to determine whether the TOE is vulnerable to Heartbleed;

c. Poodle: The objective of this test goal is to determine whether the TOE is vulnerable to Poodle;

d. Ghost: The objective of this test goal is to determine whether the TOE is vulnerable to Ghost;

e. Freak: The objective of this test goal is to determine whether the TOE is vulnerable to Freak; and

f. Shellshock: The objective of this test goal is to determine whether the TOE is vulnerable to Shellshock.

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

10.4 Conduct of Testing

HP 3PAR StoreServ Version 3.2.1 MU3 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 3PAR StoreServ Version 3.2.1 MU3 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
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
LDAP	Lightweight Directory Access Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

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. Hewlett-Packard 3PAR StoreServ Storage Systems Security Target, Version 5.0, December 07, 2015

e. Hewlett-Packard 3PAR® StoreServ Storage Systems Common Criteria EAL 2 Evaluation Technical Report, Version 0.4, December 7, 2015.