National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Pure Storage, Inc.

Pure Storage FA-405, FA-450, FlashArray//m20, FlashArray//m50, and FlashArray//m70 Series Appliances

Report Number: CCEVS-VR-10664-2016
Dated: 3/7/2016
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Jerome F. Myers, Ph.D.

The Aerospace Corporation, Columbia, MD

Kenneth B. Stutterheim

The Aerospace Corporation, Columbia, MD

Meredith M. Hennan

The Aerospace Corporation, Houston, TX

Common Criteria Testing Laboratory

Brad Mitchell, Michael Baron

InfoGard Laboratories, Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Pure Storage FlashArray 400 Series and //m Series Appliances.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The Pure Storage FlashArray and //m Series Appliances (TOE) are classified as Network Devices for the purpose of this Common Criteria evaluation. It is an enterprise Network Attached Storage solution that includes a Linux-based operating system, SAN protocols and interfaces (iSCSI, Fiber Channel, SAS), and custom software to provide network storage with high performance and reliability.

The TOE is designed to act as a data storage endpoint for a SAN. The TOE supports remote administration over HTTPS/TLS and SSH, with cryptographic encryption and authentication using CAVP validated algorithms. The TOE also supports use of external authentication and audit servers, protected using TLS.

The TOE consists of one or two physical PCs that are connected together via InfiniBand for high availability purposes. The PCs (TOE) are grouped and sold as six possible models:

- FA-405
- FA-450
- FA-m20
- FA-m50
- FA-m70

The TOE acts as a SAN storage endpoint over the Fibre Channel and 10GbE interfaces, and allows TLS connections to its 1GbE Ethernet management interface.

Table 1 below identifies components that must be present in the Operational Environment to support the operation of the TOE:

Component	Description
Syslog Server	External IT entity for audit log storage and review. • Conforms to RFC 3164 • TLS Transport Mapping – RFC 5425 • Required TLS ciphersuites (at least one of the following): TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA

	TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
NTP Server	External IT entity for accurate time accounting. • NTPv4 • Conforms to RFC 5905
Remote Console	Web Browser (the TOE is known to be compatible with the following web browsers): • Chrome 47.0-48.0 • Firefox 41.0-42.0 • Safari 6 • Protocol versions (at least one of the following): o HTTPs/TLSv1.1 (RFC 2818 & 3246) o HTTPs/TLSv1.2 (RFCs 2818 & 5246) • Ciphersuites (at least one of the following): TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 The TOE is known to be compatible with OpenSSH 6.6p1-2ubuntu2. The TOE requires an SSH client (Remote Console) supporting: Protocol versions (at least one of the following): • SSHv2 (Conforms to RFC's 4251-4254, 5656 and 6668) Data Encryption (at least one of the following):

	• AES-CBC-128 • AES-CBC-256 • AEAD_AES_128_GCM • AEAD_AES_256_GCM Data Integrity (at least one of the following): • hmac-sha1 • hmac-sha1-96 • hmac-sha2-256 • hmac-sha2-512 Key Exchange (at least one of the following): • diffie-hellman-group14-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
Local Console	• VGA monitor • USB keyboard and mouse
Ethernet	1 Gigabit Ethernet for Trusted Paths and Trusted Channels
Storage	SAS-connected SSD Storage Array from PureStorage
Authentication Server	Active Directory Authentication Server communicating via LDAP over TLS (LDAPS)
TCP Connections	The TOE's IT environment must support incoming TCP connections from the PureStorage support staff for trusted updates.

Table 1: Operational Environment Components

2 Identification of the TOE

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Pure Storage FlashArray 400 Series and //m Series Appliances

Protection Profile	• Protection Profile for Network Devices, Version 1.1, June 8, 2012 • Security Requirements for Network Devices Errata #3, November 3, 2014
Security Target	Pure Storage FlashArray Security Target, Version 1.1, March 4, 2016
Dates of Evaluation	July 17, 2015 – January 28, 2016
Conformance Result	Pass
Common Criteria Version	CC Version 3.1r3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1r3, September 2012
Evaluation Technical Report (ETR)	Common Criteria Evaluation Technical Report, 16-3399-R-0001 V1.1, March 4, 2016
Sponsor/Developer	Pure Storage, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc. NVLAP Lab Code: 100432-0
CCTL Evaluators	Brad Mitchell, Michael Baron
CCEVS Validators	Jerome F. Myers, Ph.D., Meredith M. Hennan

Table 1: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before August 28, 2015.

4 Security Policy

4.1 TOE Major Security Features Summary

- Audit
- Cryptography
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.2 Audit

The TOE audits all events and information defined by the Network Device Protection Profile v1.1. Audit logs include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event. Audit events are transmitted to an external IT entity using the TLS protocol. The TOE also protects storage of audit information from unauthorized deletion and modifications.

4.3 Cryptographic Operations

The TOE implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the SSH and TLS protocols.

The TOE zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.4 User Data Protection

The TOE ensures that any previous information content of network packets are not re-used in subsequent network packets by leveraging the Linux kernel's network packet processing mechanisms. All network resources are zeroized upon allocation of that buffer.

4.5 Identification and Authentication

The TSF supports passwords consisting of alphanumeric and all printable ASCII characters, as well as SSH public key authentication. The TSF also allows administrators to set a minimum password length and support passwords with 15 characters or more.

The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than viewing the warning banner.

4.6 Security Management

The TOE provides management over TLS, SSH, and a local console. The TOE authenticates administrative users using a username/password combination or a username/SSH_RSA key combination. The TSF does not allow access to any administrative functions prior to successful authentication. The TOE also has capability of being updated, and to verify updates via digital signature.

The TSF includes four administrative roles within the Authorized Administrator role: Internal Administrator, Array Administrator, Storage Administrator, and Read-Only Administrator. All roles are considered authorized administrators for the remainder of this document. The device ships with two hard-coded users, but allows for additional users to be authenticated through the use of Active Directory.

4.7 Protection of the TSF

The TOE uses several protection methods to ensure correct and secure operation: the TOE runs a suite of self-tests during the initial start-up (upon power on) , it provides a means to verify firmware/software updates using a digital signature mechanism prior to installing those

updates, the reading of secret and private keys is not allowed, and the TOE provides reliable time stamps for itself.

4.8 TOE Access

The TOE, for local and remote interactive sessions, terminates sessions after an Authorized Administrator-specified period of session inactivity. The TOE also allows Administrator-initiated termination of the Administrator's own interactive session.

Before establishing an administrative user session, the TOE is capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.9 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. The TOE initiates communication via the trusted channel, and also allows remote IT entities to initiate communication.

The TOE permits remote administrators to initiate a trusted path via SSH and HTTPS/TLS. The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions

	that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation. In particular, the file services provided by the models is outside the scope of this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6 Architectural Information

The TOE is classified as a Network Device for Common Criteria purposes. The TOE is made up of hardware and software components.

6.1 Architecture Overview

The TOE consists of hardware and software components.

6.1.1 TOE Hardware

- FA-405
  - PCs: 1x OEM PowerEdge R620
  - CPU: Intel Xeon E5-2640 v2, 8 cores, 2.0 GHz, 30MB Cache
  - RAM: 128 GB DDR3 1600MHz
- FA-450
  - PCs: 2x OEM PowerEdge R720
  - CPU: Intel Xeon E5-2697 v2, 12 cores, 2.7 GHz, 30MB Cache
  - RAM: 512 GB DDR3 1600MHz
- FA-m20
  - PCs: 1x Custom-built PC
  - CPU: Intel Xeon E5-2630 v3, 8 cores, 2.6 Ghz, 20MB Cache
  - RAM: 192 GB DDR4-1866
- FA-m50
  - PCs: 2x Custom-built PC
  - CPU: Intel Xeon E5-2670 v3, 12 cores, 2.3 Ghz, 25MB Cache
  - RAM: 256 GB DDR4-2133
- FA-m70
  - PCs: 2x Custom-built PC
  - CPU: Intel Xeon E5-2698 v3, 16 cores, 2.3 Ghz, 30MB Cache
  - RAM: 512 GB DDR4-2133

The TOE has the following types of physical connections:

- Host IO Cards
  - 10GbE iSCSI
  - 8GB FC
- Management Ports
  - 4x 1GbE
- Replication Ports
  - 4x 10GbE SFP
- SAS Ports
  - 8x SAS3 (12Gb/s) Mini-SAS HD
- USB Ports
  - 4x USB 3.0 Rear
  - 2x USB 2.0 Front

6.1.2 TOE Software

- Purity v4.7

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with bold titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.

7.1 Guidance Documentation

Document	Revision	Date
Guidance Documentation Pure Storage FA-400 Series and FlashArray//m Appliances Running Purity 4.7	1.3	March 4, 2016
FlashArray User Guide	1.2	January 15, 2016
FlashArray//m Quick Installation Guide	4.7.0ah	May 13, 2015
FA-450 Hardware Quick Installation Guide	N/A	August 5, 2014
FA-405 Hardware Quick Installation Guide	N/A	March 27, 2014
Purity 4.5.x Release Notes	N/A	August 10, 2015

7.2 Test Documentation

Document	Revision	Date
15-3399-R-0027 V1.2 Pure Storage Test Plan	1.3	March 4, 2016

7.3 Vulnerability Assessment Documentation

Document	Revision	Date
15-3399-R-0027 V1.2 Pure Storage Test Plan	1.3	March 4, 2016

7.4 Security Target

Document	Revision	Date
Pure Storage FlashArray Security Target	1.1	March 4, 2016

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Evaluation Team Independent Testing

The CCTL (InfoGard Laboratories, Inc.) generated the testing plan and designed the testing activities specified in the Protection Profile for Network Devices v1.1, June 8, 2012 and the Security Requirements for Network Devices Errata #3, November 3, 2014 documents, and generated automated and manual tests to execute the designed test plan. A description of the test configuration may be found in Section 5 of the 15-3399-R-0002 V1.1 Assurance Activity Report, March 4, 2016, which is publically available.

8.2 Vulnerability Analysis

All testing assurance activities and vulnerability assessment (AVA_VAN) activities were performed against the TOE by the CCTL.

The CCTL has developed a custom testing environment for ND-based evaluations which uses several virtual machines, isolated networks, and smart switches in order to meet the requirements stated by the testing assurance activities.

For the Protection Profile for Network Devices, the evaluator performed a vulnerability survey using CVEdetails.com in order to discover any publicly available exploits. The evaluator searched CVEdetails.com for the following keywords:

- Pure Storage
- Flash Array
- FlashArray
- //M
- FT-450

The evaluator also searched for the modules of OpenSSH and OpenSSL utilized by the TOE:

- OpenSSH 6.6p1-2ubuntu2
- OpenSSL FIPS Object Module 2.0.9

Only OpenSSH returned any results.

The CVE enumerated vulnerabilities that related to the installed version of OpenSSH are:

https://www.cvedetails.com/cve/CVE-2015-6564/

https://www.cvedetails.com/cve/CVE-2015-6563/

https://www.cvedetails.com/cve/CVE-2015-5600/

https://www.cvedetails.com/cve/CVE-2015-5352/

These four vulnerabilities have been addressed during the evaluation.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

InfoGard has determined that the TOE meets the security criteria in the Security Target, which claims compliance with the Protection Profile for Network Device Protection Profile, Version 1.1, June 8, 2012, and the Security Requirements for Network Devices Errata #3, November 3, 2014. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in January 2016.

10 Validator Comments/Recommendations

As noted in section 4.2 above and elsewhere, the TSF zeroizes volatile secret and private keys when power is removed. Therefore, the zeroization of these keys will cause the loss of all user data, to include all data on externally connected drives that are encrypted with AES-256.

Additionally, guidance documentation regarding the use of REST API functionality is provided with the device, however use of this functionality will take the TOE out of its evaluated configuration.

11 Security Target

Pure Storage FlashArray Security Target, Version 1.1, March 4, 2016.

12 Terms

12.1 Acronyms

CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System

IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated July 2009, Version 3.1 Revision 3, CCMB-2009-07-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[5] Protection Profile for Network Devices, June 8, 2012, Version 1.1.