Diarienummer: 23FMV4176-31

Dokument ID CSEC2023010

Swedish Certification Body for IT Security

Certification Report Dell EMC PowerStore 3.5

Issue: 1.0, 2024-mar-14

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is a secure storage system, comprised of one of the following hardware appliances:
- PowerStore 500T
- PowerStore 1200T
- PowerStore 3200T
- PowerStore 5200T
- PowerStore 9200T

with the following software:
- PowerStore OS 3.5.0.1-2083289-retail
- PSTCLI v3.5.0.891-release-x64.msi

and self encrypting drives selected from:
- Intel Optane D4800X SSD
- Intel DC SSD D7-D4512
- Kioxia CM6
- Samsung PM1723b
- Samsung PM1733

The TOE provides Network Access Server (NAS) and Storage Area Network services.

The TOE hardware is shipped directly to customers with the PowerOS installed. The software is also available for download from the Dell Digital Locker website, for registered users.

The ST does not claim conformance to any PP.

The Security Target contains four threats, two Organisational Security Policies (OSPs) and four assumptions, which have been considered during the evaluation.

The evaluation has been performed by Combitech AB in their premises in Bromma, Sweden, and in the developer's premises in Massachusetts, USA, and with assistance of EWA Canada/Intertek in their premises in Kista, Sweden. The evaluation was completed on the 5th of March 2024. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA Canada/Intertek operate as a foreign location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level: EAL 2 + ALC_FLR.2

The technical information in this report is based on the Security Target (ST) provided by the developer and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2023010
Name and version of the certified IT product	Dell EMC PowerStore 3.5 is comprised of one of the following HW appliances: - PowerStore 500T - PowerStore 1200T - PowerStore 3200T - PowerStore 5200T - PowerStore 9200T the following software: - PowerStore OS 3.5.0.1-2083289-retail - PSTCLI v3.5.0.891-release-x64.msi and one of the following self encrypting drives: - Intel Optane D4800X SSD - Intel DC SSD D7-D4512 - Kioxia CM6 - Samsung PM1723b - Samsung PM1733
Security Target	Dell PowerStore 3.5 Security Target, v0.31
EAL	EAL 2 + ALC_FLR.2
Sponsor	Dell EMC
Developer	Dell EMC
ITSEF	Combitech AB and EWA Canada/Intertek
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.5.1
Scheme Notes Release	21.0
Recognition Scope	CCRA, SOGIS, and EA/MLA
Certification date	2024-03-14

3 Security Policy

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

3.1 Security Audit

The TOE generates audit records for administrator login attempts and changes to the TOE configuration.

3.2 Cryptographic Support

Data stored on the TOE is encrypted and decrypted using FIPS 140-2 validated Self Encrypting Drives (SEDs). The relevant certificates are provided in section 7.2.

Cryptographic keys on the PowerStore are handled by the RSA BSAFE® Crypto-C Micro Edition FIPS 140-2 validated cryptographic module (certificate #4305). The associated cryptographic algorithm validation program certificate is C2130. The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

3.3 User Data Protection

The TOE only allows authorized application servers access to stored user data. The integrity of stored data is protected using RAID technology.

3.4 Identification and Authentication

TOE administrators must identify and authenticate prior to gaining access to the TOE management functionality.

3.5 Security Management

The TOE provides management capabilities via a web-based GUI and a CLI. Management functions allow authorized administrators to configure system access and storage settings.

3.6 Protection of the TSF

The TOE provides reliable time stamps for auditable events.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes four assumptions on the TOE environment.

A.ATTRIBUTE

The attributes used by the TOE to make File Storage Access Control decisions are provided by the operational environment.

A.LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.NETWORK

The network on which the TOE components are operating on is sufficiently protected from attackers.

A.NOEVIL

The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

4.2 Clarification of Scope

The Security Target contains four threats, which have been considered during the evaluation.

T.ACCESS

Access to user data could be improperly granted to application hosts which should not have access, and users with access to those hosts.

T.ACCOUNT

An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.

T.UNAUTH

A hostile/unauthorized person could gain access to stored data by bypassing the protection mechanisms of the TOE.

T.UNDETECT

Authorized users or unauthorized persons may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.PROTECT

The TOE shall incorporate mechanisms to protect against disclosure of the data it has been entrusted to store.

P.RAID

User data must be protected from loss due to disk failure.

5 Architectural Information

The TOE architecture is described in [ST] sections 1.4 and 1.5.

6 Documentation

For proper installation and configuration, the following guidance documentation is available:

Dell PowerStore 3.5 Common Criteria Guidance Supplement, version 0.7 (available upon request)

Dell PowerStore Planning Guide, May 2023

PowerStore Deployment Checklist, Rev A06

Dell PowerStore Hardware Information Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200, May 2023

Dell PowerStore Hardware Information Guide for PowerStore 500T Model, May 2023

Dell PowerStore Installation and Service Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200, May 2023

Dell PowerStore Installation and Service Guide for PowerStore 500T Model, May 2023

Dell PowerStore Networking Guide for PowerStore T Models, May 2023

Dell PowerStore T Model Software Upgrade Guide, May 2023

Dell PowerStore Security Configuration Guide, May 2023

Dell PowerStore Setting Up PowerStore Manager, May 2023

Dell PowerStore Statement of Volatility, May 2023

Dell PowerStore CLI Reference Guide, May 2023

Dell PowerStore CLI User Guide, May 2023

Dell PowerStore Configuring NFS, May 2023

Dell PowerStore Configuring SMB, May 2023

Dell PowerStore Configuring Volumes, May 2023

Dell PowerStore Monitoring Your System, May 2023

Dell PowerStore Protecting Your Data, May 2023

Dell PowerStore Release Notes for PowerStore OS Version 3.5.0.1, July 2023

Dell PowerStore Events and Alerts Reference Guide, May 2023

Dell PowerStore Power Down and Reboot Procedures Guide, May 2023

Dell PowerStore Open Source License and Copyright Information for GPLv3/LGPLv3, May 2023

Dell PowerStore Planning Guide, May 2023

7 IT Product Testing

7.1 Developer Testing

The developer tests have a good coverage of the TSF. All hardware appliances and self-encrypting drives have been fully tested. In addition, the self-encrypting drives and the embedded RSA BSAFE crypto module have been CMVP certified.

7.2 Evaluator Testing

The evaluator tested the following TOE configuration:

PowerStore 1200T

PowerStore OS 3.5.0.1-2083289-retail

PSTCLI v3.5.0.891

Samsung PM1733 Self Encrypting Drive

The evaluator tests have a good coverage of the TSF. The tests were performed remotely under close supervision by the evaluator, assisted by Dell staff.

7.3 Penetration Testing

The evaluator tested the following TOE configuration:

PowerStore 1200T

PowerStore OS 3.5.0.1-2083289-retail

PSTCLI v3.5.0.891

Samsung PM1733 Self Encrypting Drive

The evaluator penetration tests included port scans using NMAP, and a vulnerability scan using Nessus..The tests were performed remotely under close supervision by the evaluator, assisted by Dell staff. The tests contain both repeated developer tests and independent complementary tests.

8 Evaluated Configuration

The following functionality is excluded from the evaluated configuration of the TOE:

- Common Event Enabler (CEE)
- File-level retention
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Transfer Protocol (SNMP)
- Replication
- Network Data Management Protocol (NDMP)
- Distributed Hierarchical Storage Management (DHSM)
- Common Anti-Virus Agent (CAVA)
- Support Assist Enterprise (SAE)
- Express Non-Volatile Memory Non-Volatile Random Access Memory (NVMe NVRAM) – optionally used for write caching
- Common Internet File System (CIFS) support
- File transfer protocol (ftp)

The following TOE interfaces are supported, but are excluded from the evaluated configuration:

- Representational State Transfer (REST) Interface
  - Used by application developers to send HTTP operations for requests. It is not used in the evaluated configuration.
- vStorage APIs for Storage Awareness (VASA) Interface
  - Requires the installation of GUI plug-in and is not used in the evaluated configuration
- Ethernet Service Port connection
  - Ethernet Service port accessed only through the service account and is not used in the evaluated configuration
- Secure Shell (SSH) maintenance Interface
  - Disabled by default and not used in the evaluated configuration

In the evaluated configuration, the following supporting components are expected in the operational environment:

Management Workstation

Windows Server 2019 (64 bit) with Mozilla Firefox v75 or later, running on general purpose computer hardware.

LDAP Server

Windows Server 2019 with Active Directory, running on general purpose computer hardware.

NIS Server

SLES 12 SP5 with NFSv3, NFSv4, or NFSv4.1, running on general purpose computer hardware.

iSCSI Host

Windows Server 2019, running on general purpose computer hardware.

FC Host

Windows 2019, running on general purpose computer hardware.

SMB User Workstation

Windows Server 2019 with SMB 3.1.1, running on general purpose computer hardware.

NFS User Workstation

SLES 12 SP5 with NFSv3, NFSv4, or NFSv4.1, running on general purpose computer hardware.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.2	PASS
Parts of the TOE CM Coverage	ALC_CMS.2	PASS
Delivery procedures	ALC_DEL.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.2	PASS
Basic design	ADV_TDS.1	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
OSP	Organisational Security Policy
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

ST	Dell PowerStore 3.5 Security Target, Dell EMC, 2024-02-28, document version 0.31, 23FMV4176-37
AGD	Dell PowerStore 3.5 Common Criteria Guidance Supplement, Dell EMC, 2023-Dec-18, document version 0.7, 23FMV4176-11
AGD-1	Dell PowerStore Planning Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-2	PowerStore Deployment Checklist, Dell EMC, Rev A06, 23FMV4176-11
AGD-3	Dell PowerStore Hardware Information Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200, Dell EMC, May 2023, 23FMV4176-11
AGD-4	Dell PowerStore Hardware Information Guide for PowerStore 500T Model, Dell EMC, May 2023, 23FMV4176-11
AGD-5	Dell PowerStore Installation and Service Guide for PowerStore 1000, 1200, 3000, 3200, 5000, 5200, 7000, 9000, and 9200, Dell EMC, May 2023, 23FMV4176-11
AGD-6	Dell PowerStore Installation and Service Guide for PowerStore 500T Model, Dell EMC, May 2023, 23FMV4176-11
AGD-7	Dell PowerStore Networking Guide for PowerStore T Models, Dell EMC, May 2023, 23FMV4176-11
AGD-8	Dell PowerStore T Model Software Upgrade Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-9	Dell PowerStore Security Configuration Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-10	Dell PowerStore Setting Up PowerStore Manager, Dell EMC, May 2023, 23FMV4176-11
AGD-11	Dell PowerStore Statement of Volatility, Dell EMC, May 2023, 23FMV4176-11

AGD-12	Dell PowerStore CLI Reference Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-13	Dell PowerStore CLI User Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-14	Dell PowerStore Configuring NFS, Dell EMC, May 2023, 23FMV4176-11
AGD-15	Dell PowerStore Configuring SMB, Dell EMC, May 2023, 23FMV4176-11
AGD-16	Dell PowerStore Configuring Volumes, Dell EMC, May 2023, 23FMV4176-11
AGD-17	Dell PowerStore Monitoring Your System, Dell EMC, May 2023, 23FMV4176-11
AGD-18	Dell PowerStore Protecting Your Data, Dell EMC, May 2023, 23FMV4176-11
AGD-19	Dell PowerStore Release Notes for PowerStore OS Version 3.5.0.1, Dell EMC, July 2023, 23FMV4176-11
AGD-20	Dell PowerStore Events and Alerts Reference Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-21	Dell PowerStore Power Down and Reboot Procedures Guide, Dell EMC, May 2023, 23FMV4176-11
AGD-22	Dell PowerStore Open Source License and Copyright Information for GPLv3/LGPLv3, Dell EMC, May 2023, 23FMV4176-11
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CC CCpart1 + CCPart2 + CCPart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004

EP-002 002 Evaluation and Certification, CSEC, 2023-Jun-02, document version 35.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme and Scheme Notes have been used.

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was registered 2023-08-28:

QMS 2.4	valid from 2023-06-15
QMS 2.4.1	valid from 2023-09-14
QMS 2.5	valid from 2024-01-25
QMS 2.5.1	valid from 2024-02-29

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system. The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 2.5”.

The certifier concluded that, from QMS 2.4 to the current QMS 2.5.1, there are no changes with impact on the result of the certification.

A.2 Applicable Scheme Notes

SN-15 Testing

SN-18 Highlighted Requirements on the Security Target

SN-22 Vulnerability Assessment

SN-25 Use of CAVP tests in CC evaluations

SN-27 ST requirements at the time of application for certification

SN-28 Updated procedures for application, evaluation and certification