

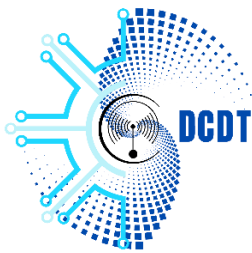
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

9 September 2026

Advisory 278: Dell PowerStore Management Interface Missing Authentication for Critical Function Vulnerability (CVE-2026-58574).

Release Date: 31st August 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate Dell PowerStore storage arrays. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-58574 (CVSS 3.1 base score 9.8, Critical, CWE-306: Missing Authentication for Critical Function) affects the management interface of Dell PowerStore. An unauthenticated remote attacker with network access to the restricted management interface can exploit the vulnerability to read internal system information directly from the appliance filesystem, with no privileges or user interaction required, potentially exposing credentials that grant full administrative access to the array.

What are the systems affected?

The following version(s) are affected:

- Dell PowerStoreT OS versions prior to 4.1.0.6-2771237 (4.1.x branch) - (Affected)
- Dell PowerStoreT OS versions prior to 4.3.1.2-2771239 (4.3.x branch) - (Affected)

Dell PowerStoreT OS 4.1.0.6-2771237 and later, or 4.3.1.2-2771239 and later - (Not affected, patched)

CERTVU confirms Dell's public security advisory (DSA-2026-330) is the authoritative source for this and the other 16 vulnerabilities it addresses; the affected and fixed version ranges above were confirmed directly against that bulletin and against Advisory 234's prior verification. Organizations should still consult the bulletin directly to confirm the correct update package for their specific PowerStore model.

What does this mean?

Typical attack flow:

1. **Reach the exposed management interface**
 - Any attacker with network access to the PowerStore array's restricted management interface - whether from within the internal network or, if misconfigured, from a wider network segment - can connect without presenting any credentials.
2. **Read internal filesystem data and harvest credentials**
 - Because the affected function performs no authentication check, the attacker can read internal system information directly from the appliance filesystem, including credentials that grant full administrative access to the array.

Attack vectors:

- A network-based, unauthenticated attack against the management interface of any reachable, unpatched Dell PowerStore array - most plausibly from an internal network segment where the management interface is reachable, but also from a wider network if the interface is inadvertently exposed.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N).

Successful exploitation may allow attackers to:

- Read internal system information and harvest administrative credentials from the PowerStore appliance filesystem without authenticating.
- Use the harvested credentials to gain full administrative access to the array, potentially exposing, modifying, or destroying any enterprise or government data it stores.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay
 - Update affected Dell PowerStoreT OS 4.1.x systems to 4.1.0.6-2771237 or later, and affected 4.3.x systems to 4.3.1.2-2771239 or later, per Dell Security Advisory DSA-2026-330.

2. Restrict network access to the management interface as defence-in-depth
3. Review the full DSA-2026-330 bulletin and Advisory 234
4. Rotate credentials after patching
5. Report suspected compromise

Report any suspected unauthorized access to a Dell PowerStore array, or any unexplained administrative account activity, to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.dell.com/support/kbdoc/en-us/000497829/dsa-2026-330-dell-powerstore-t-security-update-for-multiple-vulnerabilities>
2. <https://www.cve.org/CVERecord?id=CVE-2026-58574>