**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

2 September 2026

## Advisory 234: Dell PowerStore SDNAS Missing Authentication for Critical Function Vulnerability (CVE-2026-79687).

**Release Date:** 1st September 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 T-series storage arrays, particularly those making use of the SDNAS (file/NAS) service. This alert is intended to be understood by technical users and systems administrators.

# What is it?

CVE-2026-79687 (CVSS 3.1 base score 9.0, Critical, CWE-306: Missing Authentication for Critical Function) affects the SDNAS component of Dell PowerStore. An unauthenticated remote attacker with network access to the affected service can exploit the vulnerability to gain unauthorized filesystem access, with no privileges or user interaction required. The vulnerability's attack complexity is rated High, indicating exploitation depends on conditions not fully within the attacker's control.

CVE-2026-79687 was disclosed on 1 September 2026 in Dell Security Advisory DSA-2026-330, which addresses 17 vulnerabilities in Dell PowerStore T-series systems in total. This advisory covers CVE-2026-79687 specifically rather than the full batch. Successful exploitation could allow an attacker to read or modify data on the affected filesystem without authenticating, which for a storage array hosting shared enterprise or government data represents a significant confidentiality and integrity risk.

# What are the systems affected?

The following version(s) are affected:

- Dell PowerStoreT OS 4.1.x, versions 4.1.0.0-2435323 through 4.1.0.5-2691357 – (Affected)
- Dell PowerStoreT OS 4.3.x, versions 4.3.0.0-2611831 through 4.3.1.1-2726662 – (Affected)

Dell PowerStoreT OS 4.1.0.6-2771237 or later (fixes the 4.1.x line), and 4.3.1.2-2771239 or later (fixes the 4.3.x line) – (Not affected, patched)

CERTVU verify 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. 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 SDNAS service on an affected PowerStore array**
    - An attacker identifies a Dell PowerStore array with the SDNAS service reachable over the network, where the vulnerability's attack-complexity conditions happen to be met.
2. **Access the filesystem without authenticating**
    - The attacker exploits the missing authentication control to gain filesystem access, with no valid credentials, prior access, or user interaction required once the underlying conditions are satisfied.

**Attack vectors:**

- Network access to the SDNAS service on an affected PowerStore array - no authentication, prior access, or user interaction is required, though exploitation depends on conditions rated as High attack complexity that Dell has not further detailed.
- Particular risk where the SDNAS/NAS interface is reachable from outside a trusted storage or management network.

Successful exploitation may allow attackers to:

- Gain unauthorized read and write access to filesystem content on the affected PowerStore array.
- Compromise the confidentiality and integrity of data hosted on a shared enterprise storage platform, with downstream impact on every system or user that relies on it.

# Mitigation process

CERTVU recommends the following:

1. Apply the Dell fix 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 exposure of the SDNAS service
3. Segment storage traffic pending patching
4. Audit the estate for the affected product
5. Conduct a compromise assessment

Report suspected compromise 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-2026-79687