



CVE-2026-24505

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-24505
State	PUBLISHED
Assigner	dell
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 17:16:31 UTC
Updated	2026-04-20 19:05:30 UTC
Description	Dell PowerProtect Data Domain, versions 8.5 through 8.6 contain an improper input validation vulnerability. A high privilege

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from security_alert@emc.com

CVSS: 3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000780000 probability, percentile 0.231930000 (date 2026-04-22)

Problem Types: CWE-20 | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	security_alert@emc.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High
Availability
High
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Dell	PowerProtect Data Domain	affected 8.6.1.10, 8.7.0.0 or later semver	Not specified
CNA	Dell	PowerProtect Data Domain	affected 2.7.9 with DD OS 8.3.1.30 semver	Not specified

References			
Reference	Source	Link	Tags
www.dell.com/support/kbdoc/en-us/000450699/dsa-2026-060-security-update-fo...	security_alert@emc.com	www.dell.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

Vendor Comments And Credit

Discovery Credit

CNA: Dell would like to thank brocked200 (Nguyen Quoc Khanh) for reporting these issues.
(en)

There are currently no legacy QID mappings associated with this CVE.