



Advisory NCSC-2026-0460

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Dell PowerProtect Data Domain

Publicatiedatum: 30-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Dell heeft meerdere kritieke kwetsbaarheden verholpen in PowerProtect Data Domain, Data Domain Virtual Edition en Data Domain Management Center.

Duiding

De kritieke kwetsbaarheden met kenmerk CVE-2026-103780, CVE-2026-86384, CVE-2026-86397 en CVE-2026-86400 in Dell PowerProtect Data Domain, hebben een CVSS-score van 9.8. Een niet-geauthenticeerde kwaadwillende kan deze kwetsbaarheden op afstand misbruiken om willekeurige opdrachten uit te voeren, inloggegevens te verkrijgen of accounts met verhoogde rechten aan te maken.

Daarnaast heeft Dell drie kritieke kwetsbaarheden verholpen in Data Domain Management Center. De kwetsbaarheden met kenmerken CVE-2026-103799 en CVE-2026-103792 hebben een CVSS-score van 9.6 en CVE-2026-90717 heeft een CVSS-score van 9.1. Een kwaadwillende met beperkte gebruikersrechten kan deze kwetsbaarheden op afstand misbruiken om ongeautoriseerde toegang tot beheerde systemen te verkrijgen, handelingen uit te voeren of verhoogde rechten te verkrijgen.

Dell heeft ook verschillende andere kwetsbaarheden verholpen. Misbruik hiervan kan onder andere leiden tot het uitvoeren van willekeurige opdrachten, het verkrijgen van verhoogde rechten, ongeautoriseerde toegang tot gegevens en verstoring van de dienstverlening.

Oplossingen

Dell heeft updates uitgebracht om de kwetsbaarheden te verhelpen. De kwetsbaarheden zijn verholpen in DD OS 8.9.0.0, 7.13.1.90 (LTS2024), 8.3.1.50 (LTS2025) en 8.6.1.30 (LTS2026), of latere versies binnen de betreffende releasebranches. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.dell.com/support/kbdoc/en-us/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-68866	6.5 MEDIUM
CVE-2026-86377	7.6 HIGH
CVE-2026-86378	8.8 HIGH
CVE-2026-86379	7.2 HIGH
CVE-2026-86380	7.2 HIGH
CVE-2026-86383	6.8 MEDIUM
CVE-2026-86384	9.8 CRITICAL
CVE-2026-86385	8.8 HIGH
CVE-2026-86389	7.2 HIGH
CVE-2026-86390	6.5 MEDIUM
CVE-2026-86391	6.4 MEDIUM
CVE-2026-86393	7.2 HIGH
CVE-2026-86394	7.2 HIGH
CVE-2026-86395	7.2 HIGH
CVE-2026-86396	8.8 HIGH
CVE-2026-86397	9.8 CRITICAL
CVE-2026-86398	8.8 HIGH
CVE-2026-86399	7.2 HIGH
CVE-2026-86400	9.8 CRITICAL
CVE-2026-90717	9.1 CRITICAL
CVE-2026-90718	
CVE-2026-90720	6.7 MEDIUM
CVE-2026-90726	6.0 MEDIUM
CVE-2026-90728	6.3 MEDIUM
CVE-2026-90729	6.7 MEDIUM
CVE-2026-90730	6.5 MEDIUM
CVE-2026-94346	7.2 HIGH
CVE-2026-94347	7.2 HIGH

CVE	CVSS Score
CVE-2026-103779	8.3 HIGH
CVE-2026-103780	9.8 CRITICAL
CVE-2026-103792	9.6 CRITICAL
CVE-2026-103799	9.6 CRITICAL
CVE-2026-110540	7.1 HIGH
CVE-2026-110541	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-28	Path Traversal: '..\filedir'
CWE-31	Path Traversal: 'dir\..\filename'
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-121	Stack-based Buffer Overflow
CWE-190	Integer Overflow or Wraparound
CWE-273	Improper Check for Dropped Privileges
CWE-290	Authentication Bypass by Spoofing
CWE-306	Missing Authentication for Critical Function
CWE-321	Use of Hard-coded Cryptographic Key
CWE-354	Improper Validation of Integrity Check Value
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization

Getroffen producten

Dell
PowerProtect Data Domain
PowerProtect Data Domain Management Center
PowerProtect Data Domain Virtual Edition

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.