



NCSC-2026-0400

Dell heeft kwetsbaarheden verholpen in Container storage modules

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 05-10-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Dell heeft de kwetsbaarheden verholpen in Container Storage Modules versie 1.18.0 en hoger.

Duiding

De kwetsbaarheden bevinden zich in Dell Container Storage Modules (CSM), die worden gebruikt voor de integratie van Dell-opslagsystemen met containerplatformen zoals Kubernetes en OpenShift. De geïdentificeerde kwetsbaarheden omvatten onder meer authenticatie- en autorisatiebypasses, privilege-escalatie, informatielekken en kwetsbaarheden in CSM-componenten en CSI-drivers.

Afhankelijk van de specifieke kwetsbaarheid en de netwerkpositie en privileges van de aanvaller, kunnen aanvallers zonder authenticatie of met beperkte rechten onder andere administratieve toegang tot CSM verkrijgen, gevoelige informatie zoals Kubernetes Secrets uitlezen, RBAC-configuraties manipuleren en in het geval van bepaalde kwetsbaarheden root-level toegang tot Kubernetes-clusternodes verkrijgen. In de meest ernstige gevallen kan hierdoor de volledige CSM-omgeving en de gekoppelde storage-infrastructuur worden gecompromitteerd.

Misbruik van de kwetsbaarheden kan daarmee leiden tot een aantasting van de vertrouwelijkheid, integriteit en beschikbaarheid van getroffen Kubernetes-/OpenShift-omgevingen en de daaraan gekoppelde Dell-opslaginfrastructuur.

Oplossingen

Dell heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.dell.com/support/kbdoc/en-us/000515771/dsa-2026-448-security-update-for-dell-container-storage-modules-multiple-vulnerabilities>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-54472	
➤ CVE-2026-61411	

> CVE-2026-61421
> CVE-2026-63688
> CVE-2026-63691
> CVE-2026-63692
> CVE-2026-67269
> CVE-2026-67273
> CVE-2026-67270
> CVE-2026-70411
> CVE-2026-76105
> CVE-2026-63689
> CVE-2026-63690

CWE's

CWE	Beschrijving
> CVE-306	Missing Authentication for Critical Function
> CVE-1336	Improper Neutralization of Special Elements Used in a Template Engine
> CVE-798	Use of Hard-coded Credentials
> CVE-321	Use of Hard-coded Cryptographic Key

Getroffen producten

Dell
Container storage modules

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 of 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.