



NCSC-2026-0065

Kwetsbaarheid verholpen in Dell RecoverPoint for Virtual Machines

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-02-2026

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 een kwetsbaarheid verholpen in Dell RecoverPoint for Virtual Machines (versies voor 6.0.3.1 HF1).

Duiding

De kwetsbaarheid bevindt zich in hardcoded inloggegevens die aanwezig zijn in de software. Dit stelt ongeauthenticeerde aanvallers op hetzelfde netwerk in staat om ongeautoriseerde toegang tot het systeem te verkrijgen. Dit kan de integriteit en vertrouwelijkheid van de getroffen omgevingen in gevaar brengen.

Daarbij meldt GTIG dat zij misbruik van de desbetreffende kwetsbaarheid hebben waargenomen sinds ten minste medio 2024, dus al vóór de patch. In de bijgevoegde blogpost heeft GTIG Indicators of Compromise (IoC's) en YARA-regels opgenomen om de gebruikte malware te kunnen identificeren.

Oplossingen

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

Referenties

- <https://www.cve.org/CVERecord?id=CVE-2026-22769>
- <https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day>
- <https://www.dell.com/support/kbdoc/en-us/000426773/dsa-2026-079>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-22769	10.0 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-798	Use of Hard-coded Credentials

Getroffen producten

Dell

RecoverPoint for Virtual
Machines

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.