Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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