



NCSC-2026-0283

Kwetsbaarheden in Veeam ONE

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-08-2026

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

De kwetsbaarheden betreffen meerdere softwarecomponenten van Veeam ONE, waaronder agents en services die met verhoogde privileges draaien, evenals systemen die rapporten delen via gedeelde links en backend databases gebruiken.

Duiding

De kwetsbaarheden maken het mogelijk dat gebruikers met verschillende privilege-niveaus of zelfs onbevoegde aanvallers acties uitvoeren die normaal niet toegestaan zijn. Dit omvat het uitvoeren van willekeurige code op servers of agent hosts, het lezen van arbitraire bestanden zonder authenticatie, het omzeilen van toegangscontroles op gedeelde rapportlinks, het uitvoeren van SQL-injectieaanvallen op backend databases, en het lokaal verhogen van privileges binnen specifieke servicecontexten zoals de Reporter service. Exploitatie kan leiden tot ongeautoriseerde toegang tot gevoelige data, manipulatie van systemen, en volledige compromittering van de getroffen systemen. Sommige kwetsbaarheden vereisen lokale toegang, terwijl andere op afstand en zonder authenticatie kunnen worden misbruikt.

Oplossingen

Veeam heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.veeam.com/kb4892>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-58074	8.6 HIGH
➤ CVE-2026-58075	8.7 HIGH
➤ CVE-2026-64630	5.3 MEDIUM
➤ CVE-2026-64631	8.6 HIGH
➤ CVE-2026-64633	10.0 CRITICAL

[> CVE-2026-64634](#)

8.4 HIGH

CWE's

CWE	Beschrijving
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-269	Improper Privilege Management
> CWE-287	Improper Authentication
> CWE-863	Incorrect Authorization

Getroffen producten

Veeam

ONE

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.