Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0096

Kwetsbaarheden verholpen in Veeam Backup & Replication

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-03-2026

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

Veeam heeft kwetsbaarheden verholpen in Veeam Backup & Replication.

Duiding

De kwetsbaarheden stellen een geauthenticeerde domeingebruiker in staat om op afstand code uit te voeren op de backupserver, wat kan leiden tot ongeautoriseerde controle over backupoperaties. Dit probleem is aanwezig in de backupserveromgeving en kan worden geëxploiteerd via geauthenticeerde toegang. Daarnaast kunnen geauthenticeerde gebruikers beperkingen omzeilen en de mogelijkheid krijgen om willekeurige bestanden binnen een backuprepository te manipuleren, wat kan leiden tot gegevensmanipulatie of -corruptie. Een aanvaller met beperkte rechten kan toegang krijgen tot opgeslagen SSH-credentials, wat kan leiden tot ongeautoriseerde toegang tot kritieke systemen. De kwetsbaarheid in de hoge beschikbaarheid van Veeam Backup & Replication kan worden geëxploiteerd door een geauthenticeerde gebruiker met de rol van Backup Administrator, wat kan leiden tot compromittering van het systeem. Verder kan een aanvaller met lokale toegang zijn privileges verhogen, wat de beveiligingscontext van backup- en replicatieprocessen in gevaar kan brengen. Tot slot kan een Backup Viewer op afstand code uitvoeren met de privileges van de 'postgres'-gebruiker, wat kan leiden tot ongeautoriseerde acties binnen de databaseomgeving.

Oplossingen

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

Referenties

- https://www.veeam.com/kb4830
- https://www.veeam.com/kb4831

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-21666	9.9 CRITICAL
CVE-2026-21667	9.9 CRITICAL
CVE-2026-21668	8.8 HIGH
CVE-2026-21670	7.7 HIGH

CVE-2026-21671	9.1 CRITICAL
CVE-2026-21672	8.8 HIGH
CVE-2026-21708	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation

Getroffen producten

Veeam
Backup & Replication
Software Appliance

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.