



# NCSC-2024-0463

## Kwetsbaarheden verholpen in Veeam Backup & Replication

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 06-12-2024

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Veeam heeft kwetsbaarheden verholpen in Veeam Backup & Replication.

## Duiding

De kwetsbaarheden in Veeam Backup & Replication stellen laaggeprivilegieerde gebruikers in staat om op afstand code uit te voeren, opgeslagen referenties in platte tekst te extraheren, een agent in servermodus te starten, configuraties binnen de virtuele infrastructuur te manipuleren, en kritieke configuratie-instellingen te exploiteren. Dit kan leiden tot ongeautoriseerde toegang tot gevoelige systemen en gegevens, privilege-escalatie, en zelfs gegevensverlies. De ernst van deze kwetsbaarheden vereist een zorgvuldige beoordeling van gebruikersrechten en configuratiebeheerpraktijken door organisaties die deze software gebruiken.

## Oplossingen

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

## Referenties

➤ <https://www.veeam.com/kb4693>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2024-40717</a>	8.8 HIGH
➤ <a href="#">CVE-2024-42451</a>	7.7 HIGH
➤ <a href="#">CVE-2024-42452</a>	8.8 HIGH
➤ <a href="#">CVE-2024-42453</a>	7.4 HIGH
➤ <a href="#">CVE-2024-42455</a>	7.1 HIGH
➤ <a href="#">CVE-2024-42456</a>	8.8 HIGH
➤ <a href="#">CVE-2024-42457</a>	7.7 HIGH
➤ <a href="#">CVE-2024-45204</a>	7.7 HIGH

## CWE's

CWE	Beschrijving
> CWE-522	Insufficiently Protected Credentials
> CWE-312	Cleartext Storage of Sensitive Information
> CWE-306	Missing Authentication for Critical Function
> CWE-275	CWE-275
> CWE-862	Missing Authorization
> CWE-295	Improper Certificate Validation
> CWE-502	Deserialization of Untrusted Data
> CWE-863	Incorrect Authorization

## Getroffen producten

veeam
agent
backup___replication
backup_and_replication
veeam_backup_\&_replication

## 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.