



# NCSC-2024-0359

Kwetsbaarheden verholpen in diverse producten van Veeam.

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-10-2024

Revisie: 1.0.1

**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)

## Update Revisie 1

POC code beschikbaar, actief misbruik bekend.

## Feiten

Veeam heeft kwetsbaarheden verholpen in diverse producten, zoals Backup & Replication, ONE, Service Provider Console en Agent.

## Duiding

UPDATE: Er is inmiddels POC code online beschikbaar en CVE-2024-40711 is recentelijk actief misbruikt om ransomware uit te rollen.

Een kwaadwillende kan de kwetsbaarheden misbruiken om beveiligingsmaatregelen te omzeilen, zichzelf verhoogde rechten toe te kennen en willekeurige code uit te voeren met rechten van de applicatie.

De ernstigste kwetsbaarheid bevindt zich in Backup & Replication en heeft kenmerk CVE-2024-40711 toegewezen gekregen en stelt een ongeauthenticeerde kwaadwillende in staat om willekeurige code uit te voeren met rechten van de applicatie. Voor succesvol misbruik moet de kwaadwillende wel toegang hebben tot het kwetsbare systeem. Het is goed gebruik een dergelijke Backup & Recovery-oplossing niet publiek toegankelijk te hebben.

## Oplossingen

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

## Referenties

- <https://www.veeam.com/kb4649>
- <https://infosec.exchange/@SophosXOps/113284564225476186>
- <https://www.bleepingcomputer.com/news/security/akira-and-fog-ransomware-now-exploiting-critical-veeam-rce-flaw/>

## Kwetsbaarheden

CVE	CVSS Score
-----	------------

<a href="#">&gt; CVE-2024-38650</a>
<a href="#">&gt; CVE-2024-38651</a>
<a href="#">&gt; CVE-2024-39714</a>
<a href="#">&gt; CVE-2024-39715</a>
<a href="#">&gt; CVE-2024-39718</a>
<a href="#">&gt; CVE-2024-40709</a>
<a href="#">&gt; CVE-2024-40710</a>
<a href="#">&gt; CVE-2024-40711</a>
<a href="#">&gt; CVE-2024-40712</a>
<a href="#">&gt; CVE-2024-40713</a>
<a href="#">&gt; CVE-2024-40714</a>
<a href="#">&gt; CVE-2024-40718</a>
<a href="#">&gt; CVE-2024-42019</a>
<a href="#">&gt; CVE-2024-42020</a>
<a href="#">&gt; CVE-2024-42021</a>
<a href="#">&gt; CVE-2024-42022</a>
<a href="#">&gt; CVE-2024-42024</a>

## CWE's

<b>CWE</b>	<b>Beschrijving</b>
<a href="#">&gt; CVE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
<a href="#">&gt; CVE-22</a>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
<a href="#">&gt; CVE-275</a>	CWE-275

› CWE-284	Improper Access Control
› CWE-287	Improper Authentication
› CWE-295	Improper Certificate Validation
› CWE-434	Unrestricted Upload of File with Dangerous Type
› CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
› CWE-918	Server-Side Request Forgery (SSRF)

## Getroffen producten

<b>veeam</b>
agent
backup_&_replication
one
service_provider_console

## 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.