



NCSC-2026-0276

Kwetsbaarheden verholpen in Veeam Service Provider Console

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 05-08-2026

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

Veeam heeft meerdere kwetsbaarheden verholpen in Veeam Service Provider Console.

Duiding

De kwetsbaarheden bevinden zich in verschillende onderdelen van Veeam Service Provider Console. Een onbevoegde aanvaller kan zich voordoen als een beheerde agent binnen het systeem en daarmee de bijbehorende inloggegevens achterhalen. Daarnaast kan een aanvaller willekeurige bestanden schrijven op de managementserver, wat kan leiden tot het uitvoeren van remote code en het verkrijgen van verhoogde privileges. Verder kan een onbevoegde gebruiker een Denial-of-Service veroorzaken door overmatig geheugenverbruik te triggeren, wat de beschikbaarheid van de service beïnvloedt. Ten slotte is het mogelijk voor een onbevoegde aanvaller om tijdens de initiële fase van een beheerderssessie toegang te krijgen tot de proxied appliance API met Portal Administrator-privileges, door onvoldoende sessiebeheer en toegangscontrole.

Oplossingen

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

Referenties

➤ <https://www.veeam.com/kb4893>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-58073	9.5 CRITICAL
➤ CVE-2026-58072	9.0 CRITICAL
➤ CVE-2026-58067	8.7 HIGH
➤ CVE-2026-58071	8.2 HIGH

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-288	Authentication Bypass Using an Alternate Path or Channel
> CWE-306	Missing Authentication for Critical Function
> CWE-789	Memory Allocation with Excessive Size Value

Getroffen producten

Veeam
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.