Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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