Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

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 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
CVE-2024-40717	8.8 HIGH
CVE-2024-42451	7.7 HIGH
CVE-2024-42452	8.8 HIGH
CVE-2024-42453	7.4 HIGH
CVE-2024-42455	7.1 HIGH
CVE-2024-42456	8.8 HIGH
CVE-2024-42457	7.7 HIGH
CVE-2024-45204	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