Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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

- CVE-2024-38650
- CVE-2024-38651
- CVE-2024-39714
- CVE-2024-39715
- CVE-2024-39718
- CVE-2024-40709
- CVE-2024-40710
- CVE-2024-40711
- CVE-2024-40712
- CVE-2024-40713
- CVE-2024-40714
- CVE-2024-40718
- CVE-2024-42019
- CVE-2024-42020
- CVE-2024-42021
- CVE-2024-42022
- CVE-2024-42024

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-275	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

veeam
agent
backup_\&_replication
one
service_provider_console

Disclaimer