Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0359

Kwetsbaarheden verholpen in diverse producten van Veeam.

2024-10-11 Revisie 1

Updates

Revision: 0

Initiele versie

Revision: 1

POC code beschikbaar, actief misbruik bekend.

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

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

Interpretaties

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/