Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0232

Kwetsbaarheden verholpen in Veeam Backup Enterprise Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2024
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

Onderzoekers hebben Proof-of-Conceptcode (PoC) gepubliceerd, waarmee de kwetsbaarheid kan worden aangetoond.

Feiten

Veeam heeft kwetsbaarheden verholpen in Backup Enterprise Manager.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zonder voorafgaande authenticatie toegang te krijgen tot gebruikersaccounts die actief zijn binnen de Enterprise Manager en zo toegang te krijgen tot gevoelige gegevens binnen de context van het overgenomen account, en mogelijk willekeurige code uit te voeren met rechten van het overgenomen account.

Ondersoekers hebben Proof-of-Concept-code (PoC) gepubliceerd waarmee de kwetsbaarheid kan worden aangetoond. De werking van de PoC vereist echter dat een kwaadwillende een eigen server in de infrastructuur inbrengt, welke valselijk de Single-Sign-on overneemt, waarmee de kwaadwillende administratorrechten kan krijgen op de web-interface van Backup Enterprise Manager.

Oplossingen

Veeam heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie:

https://www.veeam.com/kb4581

Referenties

- https://www.veeam.com/kb4581

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-29852	
CVE-2024-29849	

- CVE-2024-29850
- CVE-2024-29851

CWE's

CWE	Beschrijving
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-287	Improper Authentication
CWE-294	Authentication Bypass by Capture-replay

Getroffen producten

veeam
backup_\&_replication

Disclaimer