BEACON LAB
C S I R T

CYBOLT
Security Innovation

# Boletín de Alerta

Boletín Nro.: 2024-25
Fecha de publicación: 05/09/2024
Tema: Vulnerabilidades RCE criticas en Veeam
Traffic Light Protocol (TLP): White


## Producto(s) afectado:

- Veeam Backup & Recopilation, versión 12.1.2.172 y compilaciones de la versión 12 y anteriores.
- Veeam ONE, versión 12.1.0.3208 y compilaciones de la versión 12 y anteriores.
- Veeam Service Privider Console, versión 8.1.0.213177 y compilaciones de la versión 8 y anteriores.
- Veeam Agent para Linux, versión 6.1.2.1781 y anteriores a la versión 6.
- Veeam Backup para Nutaix AHV, versión 12.5.1.8 y anteriores a la versión 12.
- Veeam Backup para Oracle Linux Virtualization Manger y Red Hat Virtualization, versión 12.4.1.45 y anteriores a la versión 12.

## Descripción

El equipo de Veeam ha publicado una serie de vulnerabilidades y sus respectivos parches de seguridad. De esta lista de vulnerabilidades podemos destacar varias que podrían afectar seriamente la seguridad de las organizaciones, como ser CVE-2024-40710 y CVE-2024-40711 que son vulnerabilidades de tipo RCE.

Hemos resaltado las mas criticas y las que consideramos que necesitan ser mitigadas lo mas pronto posible, las mismas afectan al producto **Veeam Backup & Replication:**

- **CVE-2024-40710** : Serie de vulnerabilidades que permiten la ejecución remota de código (RCE) y la extracción de datos confidenciales (credenciales y contraseñas guardadas) por parte de un usuario con pocos privilegios. (Puntuación CVSS: 8,8. Criticidad: alta).
- **CVE-2024-40713** : Los usuarios con pocos privilegios pueden modificar la configuración de autenticación multifactor (MFA) y omitirla. (Puntuación CVSS: 8,8. Criticidad: alta).
- **CVE-2024-40714** : La validación de certificados TLS débil permite la interceptación de credenciales durante operaciones de restauración en la misma red. (Puntuación CVSS: 8,3. Criticidad: alta).

- CVE-2024-39718 : Los usuarios con pocos privilegios pueden eliminar archivos de forma remota con permisos equivalentes a los de la cuenta de servicio. (Puntuación CVSS: 8,1. Criticidad: alta).
- CVE-2024-40712 : una vulnerabilidad de cruce de rutas permite que un usuario local con pocos privilegios realice una escalada de privilegios local (LPE). (Puntuación CVSS: 7,8. Criticidad: alta).
- CVE-2024-40711 : esta vulnerabilidad permita ejecución de código remoto RCE (Puntuación CVSS: 9.8, Criticidad: Critica)

También podemos entresacar algunas que afectan a los productos Veeam ONE y Veeam Service Provider Console:

- CVE-2024-42024: un atacante con credenciales de cuenta de servicio de ONE Agent puede realizar una ejecución remota de código (RCE) en la máquina host (Puntuación CVSS: 9.1, Criticidad: Critica).
- CVE-2024-38650: Esta vulnerabilidad afecta al Veeam Service Provider Console, y permite a un atacante con pocos privilegios acceder al hash NTLM de la cuenta de servicio en el servidor VSPC (Puntuación CVSS: 9.9, Criticidad: Critica)..

Si desea acceder a toda la lista de vulnerabilidad publicadas puede seguir el siguiente enlance: https://www.veeam.com/kb4649.

Recomendamos encarecidamente tomar medidas al respecto y aplicar los parches de seguridad publicados por el fabricante.

## Solución

Se han publicado parches de seguridad que mitigan dichas vulnerabilidades

- Veeam Backup & Replication 12.2 *(build 12.2.0.334)*
- Veeam Agent *for Linux* 6.2 *(build 6.2.0.101) — Included with Veeam Backup & Replication 12.2*
- Veeam ONE v12.2 *(build 12.2.0.4093)*

## Información adicional:

- https://www.veeam.com/kb4649
- https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-rce-flaw-in-backup-and-replication-software/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-40710

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com