Boletín de alerta

Boletín Nro.:
Fecha de publicación: 10/06/2026
Tema: Alerta 2026-62 Vulnerabilidad Crítica en Veeam Backup & Replication
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Veeam Backup & Replication 12.x

Descripción

Veeam publicó actualizaciones de seguridad para corregir la vulnerabilidad crítica **CVE-2026-44963** con un **CVSS v4 9.4**, la cual permite que un usuario autenticado dentro del dominio Windows ejecute código remoto (Remote Code Execution – RCE) sobre el servidor de respaldo.

Un atacante que comprometa una cuenta de dominio con privilegios limitados podría aprovechar esta falla para obtener control sobre el servidor Veeam, manipular tareas de respaldo, acceder a información sensible, alterar copias de seguridad o utilizar la plataforma comprometida como punto de apoyo para realizar movimientos laterales dentro de la red corporativa. Debido a que los servidores de respaldo suelen almacenar información crítica para la recuperación operativa, este tipo de vulnerabilidades representa un objetivo prioritario para grupos de ransomware y actores maliciosos avanzados.

Solución:

- Actualizar Veeam Backup & Replication a la versión 12.3.2.4854 o superior.

Información adicional:

- https://www.bleepingcomputer.com/news/security/new-veeam-vulnerability-exposes-backup-servers-to-rce-attacks/