Boletín de alerta

Boletín Nro.:
Fecha de publicación: 07/01/2026
Tema: Alerta 2026-01 Vulnerabilidad Crítica en Veeam Backup & Replication.
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Veeam Backup & Replication en su versión 13.0.1.180 y todas las compilaciones anteriores de la versión 13

Nota: Las versiones anteriores de Veeam Backup & Replication (es decir, 12.x y anteriores) **no** se ven afectadas por estas vulnerabilidades.

Descripción

Se identificó la vulnerabilidad **CVE-2025-59470**, la cual permite que un usuario con roles especiales de Veeam ejecute comandos maliciosos en el servidor, ya que un atacante que obtenga acceso a una cuenta con los roles de **Operador de Backup** u **Operador de Cinta** puede aprovechar parámetros manipulados para ejecutar código remotamente como el usuario interno **postgres**, lo que le permitiría ejecutar comandos en el servidor de respaldos, modificar configuraciones, manipular o borrar respaldos y utilizar el servidor como punto de entrada para otros ataques; aunque la vulnerabilidad tiene una puntuación **CVSS de 9.0 (Crítica)**, el fabricante la clasificó como **Alta** debido a que requiere el uso de roles internos altamente privilegiados.

Este tipo de vulnerabilidades suele ser aprovechado por grupos de ransomware que, una vez que logran acceso a la red, intentan manipular, deshabilitar o eliminar los respaldos con el fin de impedir la recuperación de la información y maximizar el impacto operativo, financiero y reputacional sobre la organización

La empresa también corrigió otras **tres vulnerabilidades adicionales** que afectan al mismo producto, las cuales representan riesgos relevantes para la seguridad de los sistemas:

CVE-2025-55125 (CVSS 7.2 – Alta):

Esta vulnerabilidad permite que un operador de copia de seguridad o de cinta ejecute código de forma remota (**RCE**) con privilegios de **root** mediante la creación de un archivo de configuración de respaldo malicioso. Fue descubierta durante pruebas internas y representa un riesgo elevado, ya que puede

comprometer completamente el servidor de respaldos.

CVE-2025-59469 (CVSS 7.2 – Alta):

Esta vulnerabilidad permite que un operador de copia de seguridad o de cinta escriba archivos en el sistema con privilegios de **root**, lo que podría ser utilizado para implantar malware, modificar configuraciones críticas o establecer persistencia dentro del servidor. Al igual que las anteriores, fue descubierta durante pruebas internas.

CVE-2025-59468 (CVSS 6.7 – Media):

Permite que un administrador de respaldos realice ejecución remota de código (**RCE**) como el usuario **postgres**, enviando un parámetro de contraseña manipulado. Esta falla también fue identificada durante pruebas internas y podría facilitar la escalada de privilegios o el acceso no autorizado al sistema.

Solución:

Estas vulnerabilidades se solucionaron a partir de la siguiente compilación:

- **Veeam Backup & Replication 13.0.1.1071**

Información adicional:

- **Veeam Patches Critical RCE Vulnerability with CVSS 9.0 in Backup & Replication**
- **https://www.veeam.com/kb4792**