BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-23
Fecha de publicación: 20/03/2025
Tema: Vulnerabilidad crítica RCE en Veeam Backup & Replication
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Veeam Backup & Replication versión 12.3.0.310 y todas las compilaciones anteriores a la versión 12.

Descripción

Se ha identificado una vulnerabilidad crítica en **Veeam Backup & Replication**, identificada como **CVE-2025-23120**, que permite la ejecución remota de código (**RCE**) en servidores de backup unidos a un dominio. Debido a su impacto, esta vulnerabilidad ha sido clasificada con una **gravedad crítica** y cuenta con una **puntuación CVSS v3.1 de 9.9**, lo que resalta la urgencia de aplicar las medidas de mitigación recomendadas.

Un atacante autenticado dentro del dominio podría aprovechar esta vulnerabilidad para ejecutar comandos arbitrarios con privilegios elevados, comprometiendo la integridad del sistema, afectando la disponibilidad de los respaldos y generando un riesgo significativo para la seguridad de la infraestructura. Para que esta vulnerabilidad sea explotada, el atacante debe contar con credenciales de dominio autenticadas y el servidor de backup debe estar unido a un dominio.

Solución

Se recomienda actualizar de inmediato a las versiones corregidas para mitigar riesgos de explotación:

- Versión corregida: Veeam Backup & Replication 12.3.1 (compilación 12.3.1.1139) https://www.veeam.com/kb4696

Información adicional

- https://www.veeam.com/kb4724
- https://www.rapid7.com/blog/post/2025/03/19/etr-critical-veeam-backup-and-replication-cve-2025-23120/
- https://securityonline.info/cve-2025-23120-cvss-9-9-critical-rce-vulnerability-discovered-in-veeam-backup-replication/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com