Boletín de alerta

Boletín Nro.:
Fecha de publicación: 28/05/2026
Tema: Alerta 2026-57 Vulnerabilidad en Veeam Agent
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Veeam Agent for Microsoft Windows
- Veeam Backup & Replication 13.0.1.2067 y versiones anteriores de la rama 13

Descripción

Veeam publicó actualizaciones de seguridad para corregir múltiples vulnerabilidades en Veeam Backup & Replication, destacando la vulnerabilidad CVE-2026-32996 (CVSS 7.3), una falla que permite el escalamiento local de privilegios (Local Privilege Escalation – LPE) en sistemas Windows afectados.

La vulnerabilidad afecta específicamente a Veeam Agent for Microsoft Windows y podría permitir que un atacante local con bajos privilegios obtenga permisos elevados en el sistema comprometido.

La explotación exitosa permitiría:

- Escalar privilegios locales en Windows
- Obtener control elevado sobre el host
- Manipular procesos de respaldo
- Alterar integridad de backups
- Facilitar movimientos laterales en entornos empresariales
- Desactivar controles de seguridad o recuperación

La vulnerabilidad fue reportada mediante el programa HackerOne por investigadores de Alibaba Security.

Adicionalmente, organismos de seguridad como CERT-FR emitieron alertas sobre estas vulnerabilidades debido al impacto potencial sobre la integridad de datos y plataformas de respaldo empresariales.

Aunque hasta el momento no existe confirmación pública de explotación masiva activa, las plataformas de respaldo representan objetivos prioritarios para operadores de ransomware y grupos de amenazas avanzadas debido a su capacidad para afectar recuperación operativa y continuidad de negocio.

Solución:

Se recomiendan la siguientes acciones de forma inmediata:

- Actualizar inmediatamente a Veeam Backup & Replication 13.0.2.29 o superior.
- Actualizar Veeam Agent for Microsoft Windows a las versiones corregidas publicadas por Veeam.

Información adicional:

- **Veeam Security Advisory KB4852**
- **CVE-2026-32996 – CVE.org**
- **CERT-FR Advisory CERTFR-2026-AVI-0652**
- **Vulners – CVE-2026-32996**