Veeam ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en su software Backup & Replication, la cual podría permitir la ejecución remota de código.

La falla, identificada como CVE-2025-23120, tiene una puntuación de 9.9 sobre 10 en la escala CVSS y afecta a la versión 12.3.0.310 y todas las versiones anteriores de la 12.

Según el aviso de seguridad publicado el miércoles, la vulnerabilidad permite la ejecución remota de código (RCE) a usuarios autenticados dentro del dominio.

El investigador de seguridad Piotr Bazydlo, de la firma watchTowr, ha sido reconocido por descubrir y reportar el problema, que ha sido corregido en la versión 12.3.1 (build 12.3.1.1139).

Detalles técnicos del problema

De acuerdo con Bazydlo y el investigador Sina Kheirkhah, la vulnerabilidad surge debido a una gestión inconsistente en el mecanismo de deserialización de Veeam. Específicamente, se ha identificado una clase permitida para la deserialización que, a su vez, puede desencadenar una deserialización interna, la cual usa una lista de bloqueo para evitar el procesamiento de datos considerados peligrosos.

Esto implica que un atacante podría aprovechar un elemento de deserialización que no esté incluido en la lista de bloqueo, como Veeam.Backup.EsxManager.xmlFrameworkDs y Veeam.Backup.Core.BackupSummary, para ejecutar código de manera remota.

> *«Estas vulnerabilidades pueden ser explotadas por cualquier usuario que pertenezca al grupo de usuarios locales en el servidor Windows donde se ejecuta Veeam. Aún más preocupante, si el servidor está unido a un dominio, cualquier usuario del dominio podría explotarlas»*, explicaron los investigadores.

Para mitigar el problema, Veeam ha actualizado la lista de bloqueo añadiendo los elementos

afectados. Sin embargo, si en el futuro se descubren otros elementos vulnerables no incluidos en la lista, el software podría volver a ser susceptible a ataques similares.

IBM corrige fallos críticos en AIX

Paralelamente, IBM ha lanzado actualizaciones para solucionar dos vulnerabilidades críticas en su sistema operativo AIX, las cuales podrían permitir la ejecución de comandos de manera remota.

Las vulnerabilidades afectan a las versiones 7.2 y 7.3 de AIX y han sido identificadas como:

- CVE-2024-56346 (CVSS 10.0) – Fallo de control de acceso que podría permitir a un atacante remoto ejecutar comandos arbitrarios a través del servicio nimesis NIM master.
- CVE-2024-56347 (CVSS 9.6) – Fallo de control de acceso que podría permitir la ejecución de comandos arbitrarios mediante el mecanismo de protección SSL/TLS del servicio nimsh.

Hasta el momento, no hay evidencia de que estas vulnerabilidades hayan sido explotadas activamente, pero se recomienda a los usuarios aplicar los parches de seguridad lo antes posible para evitar posibles ataques.