Splunk ha publicado actualizaciones de seguridad para corregir una vulnerabilidad crítica en Splunk Enterprise que podría ser aprovechada por atacantes para realizar operaciones de archivos sin autenticación e incluso ejecutar código de forma remota.

La falla, identificada como CVE-2026-20253, ha recibido una puntuación de 9.8 sobre 10 en el sistema de calificación CVSS.

«En las versiones de Splunk Enterprise anteriores a la 10.2.4 y 10.0.7, un usuario sin autenticación podría crear o sobrescribir archivos arbitrarios mediante un endpoint del servicio auxiliar PostgreSQL», indicó Splunk en una alerta publicada esta semana.

«La vulnerabilidad se debe a que el endpoint del servicio auxiliar PostgreSQL carece de mecanismos de autenticación, permitiendo que cualquier usuario con acceso a la red pueda ejecutar operaciones sobre archivos sin necesidad de credenciales», agregó la compañía.

El problema ha sido corregido en las siguientes versiones:

- Splunk Enterprise 10.0.0 a 10.0.6 – Solucionado en la versión 10.0.7
- Splunk Enterprise 10.2.0 a 10.2.3 – Solucionado en la versión 10.2.4
- Splunk Enterprise 10.4 – No afectado

Splunk, empresa que forma parte de Cisco, señaló que Splunk Cloud no se ve afectado por esta vulnerabilidad debido a que dicho producto no utiliza servicios auxiliares de PostgreSQL.

¿En qué consiste la vulnerabilidad?

El pasado viernes, watchTowr Labs publicó más detalles técnicos sobre CVE-2026-20253, explicando que la falla puede utilizarse para lograr ejecución remota de código previa a la autenticación en sistemas vulnerables mediante los endpoints «/v1/postgres/recovery/backup» y «/v1/postgres/recovery/restore».

La cadena de ataque funciona de la siguiente manera:

- Conectarse a una base de datos controlada por el atacante y exportar su contenido hacia un archivo arbitrario mediante el endpoint `/backup`.
- Cargar posteriormente dicho volcado en la instancia local de PostgreSQL usando el endpoint `/restore`, incluyendo un argumento denominado «passfile» que apunta a un archivo «.pgpass» («/opt/splunk/var/packages/data/postgres/.pgpass») que contiene la contraseña del usuario «postgres_admin».
- Las consultas SQL incluidas en el respaldo malicioso son ejecutadas por la instancia PostgreSQL de Splunk.

Un atacante podría explotar esta debilidad creando una función personalizada que utilice `lo_export`, una función destinada a extraer objetos binarios (BLOB) desde la base de datos y guardarlos como archivos en el sistema. De esta forma, sería posible escribir contenido arbitrario en el servidor y ejecutarlo durante el proceso de restauración.

«En este punto, podemos autenticarnos, restaurar SQL controlado por el atacante e interactuar con la base de datos local», afirmaron los investigadores de seguridad Piotr Bazydlo y Yordan Ganchev. *«Una vez que logramos restaurar SQL controlado por el atacante en la instancia local de PostgreSQL, desarrollamos rápidamente una plantilla de respaldo que nos permitió escribir archivos de manera controlada.»*

Al obtener la capacidad de escribir archivos arbitrarios dentro del sistema de archivos de Splunk, un atacante podría avanzar hacia una ejecución remota de código reemplazando scripts de Python que el producto ejecuta con frecuencia, como «/opt/splunk/etc/apps/splunk_secure_gateway/bin/ssg_enable_modular_input.py», e insertando código malicioso.

La secuencia completa del ataque sería la siguiente:

- Crear una base de datos configurada para permitir la autenticación de un usuario sin contraseña y otorgarle privilegios suficientes para ejecutar funciones como `lo_export`.
- Utilizar el endpoint `/backup` para almacenar un respaldo de la base de datos remota

dentro del sistema de archivos de Splunk.
- Emplear el endpoint `/restore` para cargar el respaldo malicioso, activar la ejecución de la función dañina durante la restauración y escribir un script Python controlado por el atacante en el servidor.

Aunque hasta el momento no existen evidencias públicas de explotación activa de esta vulnerabilidad, la divulgación de los detalles técnicos del exploit podría incentivar a actores maliciosos a lanzar campañas oportunistas contra sistemas expuestos. Por ello, resulta fundamental que las organizaciones afectadas apliquen las actualizaciones de seguridad disponibles lo antes posible para reducir el riesgo de compromiso.