

Boletín de alerta

Boletín Nro.: 105

Fecha de publicación: 21/09/2026

Tema: Alerta 2026-105 Vulnerabilidad RCE preautenticada en Splunk Enterprise

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
Splunk Enterprise	10.0.0 a 10.0.6	10.0.7 o posterior
Splunk Enterprise	10.2.0 a 10.2.3	10.2.4 o posterior
Splunk Enterprise	10.4	No afectado
Splunk Cloud Platform	No afectado	No aplica

*La vulnerabilidad afecta únicamente a Splunk Enterprise que utiliza el componente PostgreSQL *sidecar*.

Splunk Cloud Platform no está afectado, ya que no utiliza *Postgres sidecars*.

Descripción

Se identificó una vulnerabilidad etiquetada como **CVE 2026 20253**, una vulnerabilidad crítica en **Splunk Enterprise** con puntuación **CVSS 9.8**. La falla permite que un atacante remoto no autenticado realice operaciones arbitrarias sobre archivos mediante un endpoint expuesto del servicio PostgreSQL *sidecar* y, mediante una cadena de ataque, alcance **ejecución remota de código (RCE)** en el servidor Splunk.

CVE 2026 20253 se produce porque el endpoint del servicio PostgreSQL *sidecar* carece de controles de autenticación. Cualquier actor que pueda alcanzar el servicio por red puede invocar operaciones de archivo sin proporcionar credenciales. [thehackernews](https://thehackernews.com/2026/09/splunk-rce-vulnerability.html)

La vulnerabilidad permite crear o truncar archivos arbitrarios y se puede encadenar para conseguir RCE sin autenticación previa. Los endpoints implicados en la cadena técnica divulgada son:

/v1/postgres/recovery/backup
/v1/postgres/recovery/restore

El equipo de investigación demostró que un atacante puede utilizar el endpoint `/backup` para conectarse a una base de datos PostgreSQL bajo su control y guardar un *dump* en una ruta arbitraria del sistema de archivos del servidor Splunk. Posteriormente, puede invocar `/restore`, aprovechando un archivo `.pgpass`

local que contiene la contraseña de la cuenta postgres_admin, para restaurar el contenido controlado por el atacante en la instancia PostgreSQL local.

Aunque inicialmente no existían reportes de explotación, el Splunk Product Security Incident Response Team (**PSIRT**) informó el 18 de junio de 2026 que tenía conocimiento de **explotación limitada** de la vulnerabilidad. CISA añadió CVE-2026-0603 a su catálogo de vulnerabilidades explotadas conocidas (**KEV**), por lo que se recomienda priorizar la actualización inmediata y revisar posibles indicadores de compromiso.

Solución

- **Actualizar Splunk Enterprise de inmediato** a una versión corregida:
- 10.0.0–10.0.6 → actualizar a **10.0.7 o superior**.
- 10.2.0–10.2.3 → actualizar a **10.2.4 o superior**.
- Splunk Enterprise 10.4 → no afectado.

<https://advisory.splunk.com/advisories/SVD-2026-0603>

<https://docs.splunk.com/Documentation/Splunk/X/Installation/HowtoupgradeSplunk>

<https://docs.splunk.com/Documentation/Splunk/X/Admin/Serverconf>

<https://docs.splunk.com/Documentation/Splunk/X/Admin/Postgresqlconf>

- **Identificar todas las instancias Splunk Enterprise afectadas**, incluyendo *search heads*, *indexers*, nodos de administración, servidores standalone, entornos de contingencia, laboratorios y despliegues de terceros. Confirmar si cada instancia utiliza el PostgreSQL *sidecar*.
- **Restringir la exposición de los endpoints y puertos del PostgreSQL sidecar**. Limitar el acceso a redes de administración y componentes Splunk estrictamente autorizados; bloquear cualquier acceso desde Internet, redes de usuario, segmentos de invitados y VPNs no administrativas. Esta medida reduce la exposición mientras se completa el parcheo, pero no sustituye la actualización.
- **Revisar logs de red, proxy y Splunk** para detectar solicitudes HTTP sospechosas hacia:

/v1/postgres/recovery/backup

/v1/postgres/recovery/restore

- Investigar peticiones provenientes de IPs no autorizadas, patrones de respaldo/restauración no planificados o respuestas anómalas.
- **Auditar la integridad de archivos críticos de Splunk**. Verificar modificaciones recientes, especialmente en directorios de aplicaciones, scripts Python, archivos de configuración, tareas programadas, binarios, directorios temporales y rutas asociadas a la recuperación PostgreSQL.
- **Buscar persistencia y actividad posterior al compromiso**. Revisar procesos desconocidos, conexiones salientes anómalas, credenciales/tokens nuevos o modificados, cambios en roles administrativos, configuraciones de *forwarders*, alertas, *saved searches*, *lookups* y aplicaciones instaladas.

- **Rotar secretos y credenciales** si existen indicadores de compromiso. Incluir credenciales administrativas de Splunk, tokens de API, claves de despliegue, secretos de integración, certificados, credenciales de bases de datos y cuentas de servicio utilizadas por *forwarders* o conectores.

Información adicional:

- <https://thehackernews.com/2026/06/critical-splunk-enterprise-flaw-lets.html>
- <https://advisory.splunk.com/advisories/SVD-2026-0603>