Boletín de alerta

Boletín Nro.: 24
Fecha de publicación: 12/03/2026
Tema: Alerta 2026-24 Vulnerabilidad de RCE en Splunk Enterprise y Cloud
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Splunk Enterprise

- Versiones < **10.2.0**
- Versiones **10.0.0–10.0.3**
- Versiones **9.4.0–9.4.8**
- Versiones **9.3.0–9.3.9**

Splunk Cloud Platform

- Versiones < **10.2.2510.5**
- Versiones < **10.0.2503.12**
- Versiones < **10.1.2507.16**
- Versiones < **9.3.2411.124**

Descripción

Recientemente se divulgó la vulnerabilidad **CVE-2026-20163**, reportada en productos **Splunk Enterprise y Splunk Cloud Platform**, soluciones ampliamente utilizadas para la ingestión, análisis y correlación de logs y eventos de seguridad (SIEM/observabilidad). La falla posee una puntuación **CVSS v3 de 7.2 (High)** y permite que un usuario con ciertos privilegios elevados **ejecute comandos arbitrarios en el sistema subyacente**, comprometiendo potencialmente la confidencialidad, integridad y disponibilidad del entorno afectado.

El problema se origina en el endpoint REST /splunkd/__upload/indexing/preview, utilizado para la previsualización de archivos durante procesos de ingestión o indexación. Un usuario que posea un rol con la capacidad privilegiada edit_cmd puede manipular el parámetro unarchive_cmd para inyectar comandos del sistema operativo, lo que resulta en ejecución de comandos arbitrarios en el servidor Splunk.

Aunque la explotación requiere privilegios elevados dentro de la plataforma, el ataque es relativamente sencillo de ejecutar (baja complejidad) y no requiere interacción del usuario. Un atacante que comprometa una cuenta privilegiada o que abuse de configuraciones incorrectas de roles podría utilizar esta vulnerabilidad para ejecutar comandos en el host, escalar impacto dentro de la infraestructura o comprometer datos almacenados en la plataforma de análisis.

Solución y mitigaciones:

Splunk ha publicado versiones corregidas que eliminan la posibilidad de ejecutar comandos arbitrarios a través del parámetro vulnerable. Se recomienda **actualizar inmediatamente a las versiones parcheadas**:

- Splunk Enterprise **10.2.0**
- Splunk Enterprise **10.0.4**
- Splunk Enterprise **9.4.9**
- Splunk Enterprise **9.3.10**
- Versiones equivalentes corregidas en **Splunk Cloud Platform**.

En caso de que la actualización inmediata no sea posible, se recomienda implementar controles compensatorios como:

- Revisar y **restringir el uso de roles con la capacidad edit_cmd**.
- Limitar el acceso al endpoint **/splunkd/__upload/indexing/preview** únicamente a fuentes confiables.
- Monitorizar solicitudes REST que incluyan el parámetro **unarchive_cmd**.
- Revisar logs del sistema y del API en busca de **ejecución de comandos o procesos anómalos** asociados a operaciones de preview/indexing.

Adicionalmente, se recomienda habilitar monitoreo reforzado en los logs de la API REST de Splunk para detectar intentos de explotación y revisar autenticaciones o actividades sospechosas asociadas a cuentas privilegiadas.

Información adicional:

- https://advisory.splunk.com/advisories/SVD-2026-0302
- https://nvd.nist.gov/vuln/detail/CVE-2026-20163
- Splunk RCE Vulnerability Allows Attackers to Execute Arbitrary Shell Commands