Boletín de alerta

Boletín Nro.:
Fecha de publicación: 22/04/2026
Tema: Alerta 2026 -40 Vulnerabilidades Críticas en Splunk
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Splunk Enterprise

- Versiones anteriores a: 10.2.1, 10.0.5, 9.4.10 y 9.3.11

Splunk Cloud Platform

- Versiones anteriores a: 10.4.2603.0, 10.3.2512.5, 10.2.2510.9, 10.1.2507.19, 10.0.2503.13 y 9.3.2411.127

Splunk MCP Server

- Versiones anteriores a: 1.0.3

Descripción

Se han identificado vulnerabilidades de alta severidad en Splunk que permiten la exposición de tokens en texto plano (CVE-2026-20205, CVSS 7.2) y la posible ejecución remota de código por usuarios de bajo privilegio mediante la carga de archivos maliciosos (CVE-2026-20204, CVSS 7.1), afectando directamente la confidencialidad, integridad y disponibilidad de los sistemas que utilizan estas plataformas.

Las vulnerabilidades identificadas representan un riesgo significativo para la **confidencialidad, integridad y disponibilidad** de los sistemas:

- **Exposición de información sensible (CVE-2026-20205)– Riesgo: Alto (CVSS 7.2)**

Se pueden almacenar tokens de sesión y autorización en texto plano dentro de archivos de registro. Esto podría permitir que usuarios con acceso a estos registros obtengan credenciales y comprometan cuentas.

- **Ejecución remota de código (CVE-2026-20204) – Riesgo: Alto (CVSS 7.1)**
  Un atacante podría cargar archivos maliciosos aprovechando una mala gestión de archivos temporales, logrando ejecutar código en el servidor afectado.

Solución y mitigaciones:

La recomendación oficial es actualizar inmediatamente a la **última versión disponible** de los productos afectados. A continuación listamos algunos enlance que le ayudaran en el proceso.

- Guía "How to upgrade Splunk Enterprise":
  https://help.splunk.com/splunk-enterprise/administer/install-and-upgrade/9.3/upgrade-or-migrate-splunk-enterprise/how-to-upgrade-splunk-enterprise
  Ahí está el paso a paso (backups, orden de actualización, chequeos posteriores, etc.).

- Portal general de documentación de Splunk:
  https://help.splunk.com

Información adicional:

- https://advisory.splunk.com/advisories
- https://advisory.splunk.com/advisories/SVD-2026-0407
- https://advisory.splunk.com/advisories/SVD-2026-0403