Alerta de seguridad cibernética	9VSA24-00963-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	23 de enero de 2024
Última revisión	23 de enero de 2024

NOTIFICACIÓN: La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de varios parches publicados por Splunk para diversos productos, incluyendo una de alta severidad.

Vulnerabilidades

CVE-2024-23675
CVE-2024-23676
CVE-2024-23677
CVE-2024-23678

Impacto

Vulnerabilidades de riesgo alto:

CVE-2024-23678: Vulnerabilidad que resulta en la deserialización insegura de datos no confiables desde una partición separada de disco en la máquina. Esto podría provocar denegación de servicio o ejecución de código arbitrario. CVSS: 7.5.

Mitigación

Actualizar a Splunk Enterprise 9.0.8, 9.1.3 o superiores.

Productos afectados

Splunk Enterprise for Windows.

Enlaces

https://advisory.splunk.com/advisories/SVD-2024-0108
https://advisory.splunk.com/advisories

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.23 12:47:46 -03'00'