Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00661-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2022
Última revisión	17 de junio de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre una nueva vulnerabilidad en Splunk Enterprise.

Vulnerabilidades

CVE-2022-32158

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2022-32158: Esta vulnerabilidad puede permitir a un atacante comprometer un endpoint Universal Forwarder y luego usarlo para la ejecución arbitraria de código en otros endpoints conectados al servidor.

Productos afectados

Splunk Enterprise anteriores a la versión 9.0.

La Splunk Cloud Platform (SCP) no es afectada por esta vulnerabilidad.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.splunk.com/en_us/product-security.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32158

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.17 14:39:49 -04'00'