Alerta de seguridad cibernética	9VSA22-00620-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2022
Última revisión	14 de abril 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 del Gobierno de Chile, CSIRT de Gobierno, advierte sobre una vulnerabilidad crítica que debe ser remediada cuanto antes, y que afecta al framework Struts de Apache.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-31805

Impacto

La vulnerabilidad es considerada **crítica**. Ocurre debido a un error de inyección OGNL que puede llevar a la ejecución remota de código (RCE). Este problema se creía resuelto con una actualización de 2020, pero recientemente se descubrió que el error aún puede ser explotado, por lo que entidades como la CISA de Estados Unidos instan a actualizar a la versión 2.5.30 o superiores.

Productos afectados

Apache Struts 2 2.0.0 a 2.5.29 (inclusive)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor (versión 2.5.30 y superiores).

Enlaces

https://cwiki.apache.org/confluence/display/WW/S2-062

https://www.cisa.gov/uscert/ncas/current-activity/2022/04/12/apache-releases-security-advisory-struts-2
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31805

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.14 17:02:06 -04'00'