Alerta de seguridad cibernética	9VSA23-00796-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	22 de febrero de 2023
Última revisión	22 de febrero de 2023

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, comparte información sobre una vulnerabilidad en FortiAnalyzer.

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

Vulnerabilidad

CVE-2022-30304

Impacto

Esta vulnerabilidad puede permitir que un atacante remoto no autenticado realice un ataque de secuencias de comandos cruzadas (XSS) almacenadas a través del parámetro de URL observado en la vista de registro de eventos de ataque de FortiWeb en FortiAnalyzer.

Productos afectados

FortiAnalyzer versión 7.2.0 a 7.2.1.
FortiAnalyzer versión 7.0.0 a 7.0.4
FortiAnalyzer versión 6.4.0 a 6.4.8
FortiAnalyzer versión 6.2.0 a 6.2.9
FortiAnalyzer versión 6.0.0 a 6.0.11

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-22-166
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30304

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.23 12:48:09 -03'00'