Alerta de seguridad cibernética	9VSA23-00793-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de febrero de 2023
Última revisión	20 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 crítica en FortiNAC.

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

Vulnerabilidad

CVE-2022-39952

Impacto

Un control externo de vulnerabilidad de ruta o nombre de archivo [CWE-73] en el servidor web de FortiNAC puede permitir que un atacante no autenticado realice una escritura arbitraria en el sistema.

Productos afectados

FortiNAC versión 9.4.0
FortiNAC versión 9.2.0 a 9.2.5
FortiNAC versión 9.1.0 a 9.1.7
FortiNAC 8.8 todas las versiones
FortiNAC 8.7 todas las versiones
FortiNAC 8.6 todas las versiones
FortiNAC 8.5 todas las versiones
FortiNAC 8.3 todas las versiones

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-22-300
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39952