Alerta de seguridad cibernética	9VSA22-00748-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	24 de noviembre de 2022
Última revisión	24 de noviembre 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 CSIRT de Gobierno comparte información entregada por Fortinet sobre una vulnerabilidad que afectan a algunos de sus productos, y que la empresa conoce ya ha sido explotada.

Vulnerabilidades

CVE-2022-40684

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-40684: Bypass de autenticación (CWE-288) en FortiOS, FortiProxy y FortiSwitchManager, puede permitir a un atacante no autenticado realizar operaciones en la interfaz de administración a través de solicitudes HTTP o HTTPS especialmente diseñadas.

Productos afectados

FortiOS: 7.0.0 a 7.2.1.
FortiProxy: 7.0.0 a 7.2.0.
FortiSwitchManager: 7.2.0, 7.0.0

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-22-377
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.24 17:30:25 -03'00'

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob