Alerta de seguridad cibernética	9VSA23-00944-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2024
Última revisión	4 de enero de 2024

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 sobre una vulnerabilidad de riesgo alto que afecta a FortiOS, FortiProxy y FortiPAM.

Vulnerabilidades

CVE-2023-36639

Impacto

Vulnerabilidades de riesgo alto:

CVE-2023-36639: Vulnerabilidad de formato de cadenas (CWE.134) en el Daemon HTTPSd de FortiOS, FortiProxy y FortiPAM, que podría permitir a un usuario no autenticado ejecutar código no autorizado o comandos a través de solicitudes API especialmente diseñadas. CVSSv3: 7.

Mitigación

Actualizar según su producto a una versión actualizada siguiendo lo indicado por Fortinet aquí:
https://docs.fortinet.com/upgrade-tool

Productos afectados

FortiProxy 7.2.0 a 7.2.4 y 7.0.0 a 7.0.10
FortiOS: 7.4.0, 7.2.0 a 7.2.4 y 7.0.0 a 7.0.11, 6.4.0 a 6.4.12, 6.2.0 a 6.2.15. 6.0.0 a 6.0.17
FortiPAM: 1.0.0 a 1.0.3

Enlaces

https://www.fortiguard.com/psirt/FG-IR-23-138
https://cwe.mitre.org/data/definitions/134.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.04 17:05:06 -03'00'