

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00858-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de julio de 2023
Última revisión	11 de julio 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 afectada a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información de nuevas vulnerabilidades parchadas por Fortinet para FortiOS y FortiProxy.

Vulnerabilidades

CVE-2023-33308

CVE-2023-33306

CVE-2023-28001

CVE-2023-27997

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-33308: Vulnerabilidad de desborde stack-based, que afecta la función de inspección profunda en modo proxy en FortiOS y FortiProxy, que puede permitir a un atacante remoto ejecutar código arbitrario o comandos. CVSSv3: 9.8.

CVE-2023-27997: Vulnerabilidad de desborde heap-based en FortiOS y FortiProxy SSL-VPN, permite a un atacante remoto ejecutar código arbitrario o comandos a través de solicitudes especialmente diseñadas. CVSSv3: 9.2.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

FortiOS-6K7K 7.0.5 a 6.0.10.

FortiOS: 7.2.4 a 6.0.0.

FortiProxy 7.2.3 a 1.1.0.

Enlaces

<https://www.fortiguard.com/psirt/FG-IR-23-183>

<https://www.fortiguard.com/psirt/FG-IR-23-097>

<https://www.fortiguard.com/psirt/FG-IR-23-028>

<https://www.fortiguard.com/psirt/FG-IR-23-015>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33308>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33306>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28001>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27997>