

# 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	9VSA23-00846-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de junio de 2023
Última revisión	12 de junio 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 una vulnerabilidad crítica parchada por Fortinet para su producto FortiGate SSL.

## Vulnerabilidades

CVE-2023-27997

## Impacto

### Vulnerabilidades de riesgo crítico

CVE-2023-27997: Vulnerabilidad que afecta todos las VPN SSL y que puede ser explotada para lograr ejecución remota de código sin autenticación.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Productos afectados

FortiGate SSL. Según la información conocida al momento de publicar este documento (no ha habido aún información oficial desde Fortinet) el parche estará disponible en FortiOS 7.0.12, 7.2.5, 6.4.13 y 6.2.15.

### Enlaces

<https://olympcyberdefense.fr/1193-2/>

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