

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	9VSA22-00760-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero 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 sobre vulnerabilidades recientemente dadas a conocer por Fortinet para sus productos FortiADC y FortiTester.

Vulnerabilidades

CVE-2022-39947
CVE-2022-35845

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-39947: Una neutralización inapropiada de elementos especiales en una vulnerabilidad OS Command en FortiADC puede permitir a un atacante autenticado con acceso al GUI web ejecutar código no autorizado o comandos a través de solicitudes HTTP especialmente diseñados.

CVE-2022-35845: Varias neutralizaciones inapropiadas de elementos especiales usados en vulnerabilidades OS Command en FortiTester podría permitir a un atacante autenticado ejecutar comandos arbitrarios en la shell subyacente.

Productos afectados

FortiADC versión 7.0.0 a 7.0.2
FortiADC versión 6.2.0 a 6.2.3
FortiADC versión 6.1.0 a 6.1.6
FortiADC versión 6.0.0 a 6.0.4
FortiADC versión 5.4.0 a 5.4.5
FortiTester versión 7.1.0
FortiTester versión 7.0 todas
FortiTester versión 4.0.0 a 4.2.0
FortiTester versión 2.3.0 a 3.9.1

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>

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://www.fortiguard.com/psirt/FG-IR-22-061>

<https://www.fortiguard.com/psirt/FG-IR-22-274>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39947>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35845>