

# 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	9VSA22-00744-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de noviembre de 2022
Última revisión	15 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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información entregada por Cisco sobre vulnerabilidades en varios de sus productos.

## Vulnerabilidades

CVE-2022-20947	CVE-2022-20925	CVE-2022-20831	CVE-2022-20843
CVE-2022-20946	CVE-2022-20926	CVE-2022-20832	CVE-2022-20872
CVE-2022-20924	CVE-2022-20934	CVE-2022-20833	CVE-2022-20905
CVE-2022-20927	CVE-2022-20928	CVE-2022-20834	CVE-2022-20932
CVE-2022-20745	CVE-2022-20950	CVE-2022-20835	CVE-2022-20935
CVE-2022-20854	CVE-2022-20922	CVE-2022-20836	CVE-2022-20936
CVE-2022-20918	CVE-2022-20943	CVE-2022-20838	CVE-2022-20713
CVE-2022-20826	CVE-2022-20941	CVE-2022-20839	CVE-2022-20938
CVE-2022-20949	CVE-2022-20940	CVE-2022-20840	

## Impacto

### Vulnerabilidades de mayor riesgo

CVE-2022-20927: Error en la función Dynamic Access Policies (DAP) del software ASA y FTD, permite a un atacante remoto no autenticado provocar una condición de denegación de servicio (DoS).

CVE-2022-20946: Vulnerabilidad de denegación de servicio (DoS) en el GRE tunnel decapsulation feature de FTD.

### Productos afectados

Cisco Firepower Threat Defense Software  
Cisco Firepower Threat Defense Software  
Cisco Firepower Management Center Software

## 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://twitter.com/csirtgob)

<https://www.linkedin.com/company/csirt-gob>

Cisco Firepower Software for ASA Firepower Module  
Cisco Adaptive Security Appliance Software  
Cisco NGIPS Software  
Cisco Secure Firewall 3100 Series

## Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

## Enlaces

<https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74838>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20947>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20946>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20924>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20927>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20745>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20854>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20918>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20826>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20949>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20925>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20926>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20934>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20928>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20950>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20922>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20943>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20941>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20940>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20831>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20832>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20833>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20834>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20835>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20836>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20838>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20839>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20840>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20843>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20872>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20905>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20932>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20932>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20936>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20713>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20938>