Alerta de seguridad cibernética	9VSA22-00626-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2022
Última revisión	28 de abril 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre dos nuevas vulnerabilidades comunicadas por Cisco para varios de sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-20746
CVE-2022-20751
CVE-2022-20757
CVE-2022-20743
CVE-2022-20759
CVE-2022-20742
CVE-2022-20745
CVE-2022-20760
CVE-2022-20737
CVE-2022-20715
CVE-2022-20767
CVE-2022-20681
CVE-2022-20729
CVE-2022-20730
CVE-2022-20748
CVE-2022-20627
CVE-2022-20628
CVE-2022-20629
CVE-2022-20740
CVE-2022-20744

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-20746: Denegación de servicio.
CVE-2022-20751: Denegación de servicio.
CVE-2022-20757: Denegación de servicio.
CVE-2022-20743: Bypass de seguridad.
CVE-2022-20742: Divulgación de información.
CVE-2022-20745: Denegación de servicio.
CVE-2022-20760: Denegación de servicio.

CVE-2022-20737: Desbordamiento de lotes.
CVE-2022-20715: Denegación de servicio.

Productos afectados

Cisco Firepower Threat Defense Software TCP Proxy.
Cisco Firepower Threat Defense Software Snort.
Cisco Firepower Threat Defense Software.
Cisco Firepower Management Center File Upload.
Cisco Adaptive Security Appliance Software
Cisco Firepower Threat Defense (FTD) Software.
Cisco Adaptive Security Appliance (ASA) Software.
Cisco Firepower Management Center (FMC) Software.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-kM9SHhOu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-dos-hd2hFgM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-JnnJm4wB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-security-bypass-JhOd29Gg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ipsec-mitm-CKnLr4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-nJVAwOeq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-tzPSYern
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssl-vpn-heap-zLX3FdX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FTD-snort3-DOS-Aq38LVdM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-priv-esc-ybvHKO5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-xmlinj-8GWjGzKe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-sidns-bypass-3PzA5pO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-amp-local-dos-CUfwRJXT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-qXz4uAkM

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-SfpEcvGT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-infdisc-guJWRwQu
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20681
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20730
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20627
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20628
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20744

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.28 12:45:19 -04'00'