Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00643-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 de mayo 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 sobre vulnerabilidades que afectan a diversos productos de Cisco.

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

Vulnerabilidades

CVE-2022-20797
CVE-2022-20806
CVE-2022-20807
CVE-2022-20809
CVE-2022-20802
CVE-2022-20666
CVE-2022-20667
CVE-2022-20668
CVE-2022-20765
CVE-2022-20759
CVE-2022-20681
CVE-2022-20677
CVE-2022-20718
CVE-2022-20719
CVE-2022-20720
CVE-2022-20721
CVE-2022-20722
CVE-2022-20723
CVE-2022-20724
CVE-2022-20725
CVE-2022-20726
CVE-2022-20727

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-20759: Vulnerabilidad en las interfaces web de las funcionalidades VPN de Cisco Adaptive Security Appliance (ASA) software y Cisco Firepower Threat Defense (FTD) software podría permitir a un atacante remoto autenticado pero sin privilegios elevar sus privilegios hasta el nivel 15.

CVE-2022-20681: Vulnerabilidad en el CLI de Cisco IOS XE Software for Cisco Catalyst 9000 Family Switches y Cisco Catalyst 9000 Family Wireless Controllers podría permitir a un atacante local autenticado elevar privilegios al nivel 15 en un aparato afectado.

Productos afectados

Cisco Secure Network Analytics anteriores a 7.4.1.
Cisco Expressway Series y Cisco TelePresence VCS 14.0 y anteriores.
Cisco Enterprise Chat and Email (ECE) anteriores a 12.6(1) ES2.
Cisco CSPC 2.10.0.2 y anteriores.
Cisco ASA software anteriores a 9.12.4.38, 9.14.4, 9.15.1.21, 9.16.2.14 y 9.17.7.
Cisco FMC y FTD software anteriores a 6.4.0.15, 6.6.5.2, 7.0.2 y 7.1.0.1.
800 Series Industrial Integrated Services Routers (Industrial ISRs)
800 Series Integrated Services Routers (ISRs)
1000 Series Connected Grid Router (CGR1000) Compute Modules
IC3000 Industrial Compute Gateways
Industrial Ethernet (IE) 4000 Series Switches
IOS XE-based devices configured with IOx
IR510 WPAN Industrial Routers

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hYb9KFK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-filewrite-bsFVwueV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-strd-xss-BqFXO9D2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-multi-xss-tyDFjhwb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-mgmt-privesc-BMFMUvye
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-priv-esc-ybvHKO5
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-yuXQ6hFj
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20809
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20802
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20666
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20667
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20668
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20765

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20677
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20718
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20719
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20721
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20722
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20724
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20725
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20726
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20727
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20681