Alerta de seguridad cibernética	9VSA22-00687-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2022
Última revisión	10 de agosto 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 algunos productos de Cisco.

Vulnerabilidades

CVE-2022-20798
CVE-2022-20869
CVE-2022-20816
CVE-2022-20914
CVE-2022-20820
CVE-2022-20852
CVE-2022-20827
CVE-2022-20841
CVE-2022-20842
CVE-2021-1585
CVE-2022-20713
CVE-2022-20829
CVE-2022-20866
CVE-2022-20715

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-20798: Vulnerabilidad en la función de autenticación externa de Cisco Secure Email y Web Manager, podría permitir a un atacante remoto no autenticado evadir la autenticación y hacer login en la interfaz de administración web en el dispositivo afectado.

CVE-2022-20842, CVE-2022-20827 y CVE-2022-20841: Vulnerabilidad en routers Cisco Small Business RV160, RV260, RV340 y RV345 podría permitir a un atacante remoto no autenticado ejecutar código arbitrario o causar denegación de servicio (DoS) en el aparato afectado.

Productos afectados

RV160 VPN Routers
RV160W Wireless-AC VPN Routers
RV260 VPN Routers
RV260P VPN Routers with PoE

RV260W Wireless-AC VPN Routers
RV340 Dual WAN Gigabit VPN Routers
RV340W Dual WAN Gigabit Wireless-AC VPN Routers
RV345 Dual WAN Gigabit VPN Routers
RV345P Dual WAN Gigabit POE VPN Routers
Cisco Secure Email and Web Manager
Cisco ASA Software Release
Cisco FTD Software Release
ASA 5506-X with FirePOWER Services
ASA 5506H-X with FirePOWER Services
ASA 5506W-X with FirePOWER Services
ASA 5508-X with FirePOWER Services
ASA 5516-X with FirePOWER Services
Firepower 1000 Series Next-Generation Firewall
Firepower 2100 Series Security Appliances
Firepower 4100 Series Security Appliances
Firepower 9300 Series Security Appliances
Secure Firewall 3100
Aparatos Cisco si corren una edición del Cisco ASA Software anterior a la 9.17(1) y tienen activado Clientless SSL VPN
Aparatos Cisco si corren una edición del Cisco ASA Software anterior a 9.16.3.19, 9.17.1.13, o 9.18.2., el aparato está configurado con una versión Cisco ASDM anterior a la 7.18.1.152., la imagen Cisco ASDM usa un lCisco ASDM-IDM Launcher anterior a la versión 1.9(5) y el aparato está configurado para acceso de administración HTTPS
Cisco ASDM, ediciones anteriores a 7.18.1.152
Cisco Webex Meetings
Cisco Identity Service Engine (ISE) Software
Cisco Unified CM y Cisco Unified CM SME
Cisco BroadWorks Application Delivery Platform Software

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/publicationListing.x
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20798
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20869
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20816
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20914
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20820
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20842
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1585

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20713
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20866
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20715

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.10 17:38:02 -04'00'