Alerta de seguridad cibernética	9VSA22-00741-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de noviembre de 2022
Última revisión	09 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 varias vulnerabilidades que afectan a algunos de sus productos.

Vulnerabilidades

CVE-2022-20867
CVE-2022-20868
CVE-2022-20961
CVE-2022-20956
CVE-2022-20951
CVE-2022-20958

Impacto

Vulnerabilidades de riesgo alto

CVE-2022-20867 y CVE-2022-20868: Vulnerabilidades en la interfaz UI de próxima generación de Cisco Email Security Appliance (ESA), Cisco Secure Email and Web Manager, y Cisco Secure Web Appliance, antes conocida como Cisco Web Security Appliance (WSA), podrían permitir a un atacante elevar privilegios o realizar una inyección SQL y obtener privilegios root.

CVE-2022-20961: Vulnerabilidad en la interfaz de administración web de Cisco Identity Services Engine (ISE), podría permitir a un atacante remoto no autenticado realizar un ataque CSRF y ejecutar acciones arbitrarias en un equipo afectado. Ocurre debido a protecciones CSRF insuficientes.

CVE-2022-20956: Vulnerabilidad en la interfaz de administración web de Cisco Identity Services Engine (ISE), podría permitir a un atacante remoto no autenticado realizar un ataque CSRF y ejecutar acciones arbitrarias en un equipo afectado, debido a un control inapropiado de acceso.

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

CVE-2022-20951 y CVE-2022-20958: Vulnerabilidades en la interfaz de administración web de Cisco BroadWorks CommPilot Application Software podrían permitir a un atacante remoto autenticado ejecutar código arbitrario en un dispositivo afectado u obtener información confidencial desde el servidor Cisco BroadWorks u otros aparatos en la red.

Productos afectados

Cisco ESA
Cisco Secure Email and Web Manager
Cisco Secure Web Appliance
Cisco Identity Services Engine (ISE)
Cisco BroadWorks CommPilot Application 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-2022-20867
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20958