Alerta de seguridad cibernética	9VSA24-00973-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	6 de febrero de 2024
Última revisión	6 de febrero de 2024

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 CSIRT de Gobierno comparte información de vulnerabilidades críticas que afectan a Cisco Expressway Series, para los cuales la empresa ya ha publicado parches.

Vulnerabilidades

CVE-2024-20252 CVE-2024-20254 CVE-2024-20255

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2024-20252 y CVE-2024-20254: Vulnerabilidades que podrían permitir a un atacante no autenticado y remoto realizar un ataque de tipo cross-site request forgery (CSRF), que podrían permitir al atacante realizar acciones arbitrarias en un dispositivo afectado. CVSS: 9.6.

Mitigación

Para Cisco Expressway Series 14.0, instalar la versión 14.3.4 o posteriores.
Para Cisco Expressway Series 15.0, instalar la versión 15.0.0 o posteriores.
Para versiones anteriores a la 14.0, cambiar por una versión corregida.

Productos afectados

Cisco Expressway Series Release.

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-KnnZDMj3

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.02.08 15:29:56 -03'00'