

Alerta de seguridad cibernética	9VSA22-00560-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2022
Última revisión	24 de enero 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 equipo CSIRT. 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 vulnerabilidad en Cisco Webex Meetings.

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

Vulnerabilidades

CVE-2022-20654

Impactos

Vulnerabilidad de riesgo medio

CVE-CVE-2022-20654: Un atacante remoto puede engañar a la víctima para que siga un enlace especialmente diseñado y ejecute código HTML y script arbitrario en el navegador del usuario en el contexto de un sitio web vulnerable. La explotación exitosa de esta vulnerabilidad puede permitir que un atacante remoto robe información potencialmente confidencial, cambie la apariencia de la página web, realice ataques de phishing y de descarga oculta.

Productos afectados

Todas las versiones de Cisco Webex Meetings.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-FmbPu2pe>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20654>