Alerta de seguridad cibernética	9VSA24-00952-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2024
Última revisión	11 de enero 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 una vulnerabilidad parchada por Cisco para su producto Unity Connection.

Vulnerabilidades

CVE-2024-20272

Impacto

Vulnerabilidades de riesgo alto:

CVE-2024-20272: Vulnerabilidad en la interfaz de administración basada en la web de Cisco Unity Connection podría permitir a un atacante remoto no autenticado a cargar archivos arbitrarios a un sistema afectado y ejecutar comandos en el sistema operativo subyacente. CVSS 7.3 base.

Mitigación

Implementar las versiones parchadas de Cisco Unity Connection. Para las versiones 12.5 y anteriores, la primera versión parchada es la 12.5.1.19017-4, mientras para la versión 14, la primera versión parchada es la 14.0.1.14006-5. Para conseguirlas se debe contactar al Cisco TAC.

Productos afectados

Cisco Unity Connection 14, 12.5 y anteriores.

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.11 11:39:12 -03'00'