Alerta de seguridad cibernética	9VSA24-00970-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2024
Última revisión	30 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 crítica en varios productos de Cisco Unified Communications y Cisco Contact Center Solutions.

Vulnerabilidades

CVE-2024-20253

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2024-20253: Vulnerabilidad que podría ser explotada por un atacante, al enviar un mensaje a un dispositivo afectado, para ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario de servicios web. CVSS: 9.9.

Mitigación

Implementar las actualizaciones de software disponibles en el siguiente enlace:
https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

Productos afectados

Los siguientes productos en la configuración por defecto:
Unified Communications Manager (Unified CM) (CSCwd64245)
Unified Communications Manager IM & Presence Service (Unified CM IM&P) (CSCwd64276)
Unified Communications Manager Session Management Edition (Unified CM SME) (CSCwd64245)
Unified Contact Center Express (UCCX) (CSCwe18773)
Unity Connection (CSCwd64292)
Virtualized Voice Browser (VVB) (CSCwe18840)

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.30 16:23:48 -03'00'

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm