Alerta de seguridad cibernética	9VSA21-00509-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2021
Última revisión	21 de octubre de 2021

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 vulnerabilidades recientemente publicadas por Oracle.

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

Vulnerabilidades

CVE-2021-1529
CVE-2021-34737
CVE-2021-34743
CVE-2021-34760
CVE-2021-34789
CVE-2021-34738
CVE-2021-40121
CVE-2021-40123
CVE-2021-34736
CVE-2021-40122

Impactos

Vulnerabilidades de riesgo alto:

CVE-2021-1529: Vulnerabilidad de inyección de comandos en Cisco IOS XE SD-WAN y en productos que estén usando Cisco IOS XE Software en modo Controller, debida a una validación insuficiente de inputs en el CLI del sistema, y que permite a un atacante local no autenticado ejecutar comandos arbitrarios con privilegios de root.

Productos Afectados

Cisco IOS XE SD-WAN
Cisco IOS XE Software
Cisco Webex Software

Cisco IOS XR Software 6.7.2 y posteriores, 7.1.2 y posteriores, y 7.2.1 y posteriores pero anteriores al 7.3.2
Cisco TMS Software
Cisco Tetration
Cisco ISE Software
UCS C-Series Rack Servers in standalone mode
UCS S-Series Storage Servers in standalone mode
Cisco Meeting Server

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-rhpbE34A
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-pjPVReLU
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-2FmKd7T
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-CwjZJSQc
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sec-work-xss-t6SYtu8Q
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss1-rgxYry2V
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-download-B3BR5KQA
tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-gui-dos-TZjrFyZh
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1529
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34738
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40121
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34736
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40122

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.21 12:09:19 -03'00'