Alerta de seguridad cibernética	9VSA21-00419-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2021
Última revisión	11 de abril 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, CSIRT, comparte información sobre vulnerabilidades en distintos productos de Cisco.

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

Vulnerabilidades

CVE-2021-3449
CVE-2021-3450
CVE-2021-1137
CVE-2021-1479
CVE-2021-1480
CVE-2021-1459
CVE-2021-1472
CVE-2021-1473
CVE-2021-1251
CVE-2021-1308
CVE-2021-1309
CVE-2021-1362
CVE-2021-1386
CVE-2021-1485
CVE-2021-1467
CVE-2021-1420
CVE-2021-1474
CVE-2021-1475
CVE-2021-1413
CVE-2021-1414
CVE-2021-1415
CVE-2021-1463
CVE-2021-1380
CVE-2021-1407
CVE-2021-1408
CVE-2021-1399
CVE-2021-1406

Impactos

Como vulnerabilidades de riesgo **crítico** son calificadas las siguientes:

CVE-2021-1137, CVE-2021-1479, CVE-2021-1480 afectan al Cisco SD-WAN vManage Software. Estas vulnerabilidades podrían permitir a un atacante remoto no autenticado ejecutar código arbitrario o permitir a un atacante local, autenticado, escalar privilegios en un sistema afectado.

CVE-2021-1459 afecta a las interfaces de administración de los routers Cisco Small Business RV110W, RV130, RV130W, and RV215W. Esta vulnerabilidad podría permitir a un atacante remoto no autenticado el ejecutar código arbitrario en un aparato afectado.

Como vulnerabilidades de riesgo **alto** son calificadas las siguientes:

CVE-2021-1472 y CVE-2021-1473 afectan a la interfaz web de los routers Cisco Small Business RV Series. Un atacante remoto podría ejecutar comandos arbitrarios o evadir la autenticación y subir archivos a un aparato afectado.

CVE-2021-1251, CVE-2021-1308 y CVE-2021-1309 son vulnerabilidades existentes en la implementación del Link Layer Discovery Protocol (LLDP) de los routers Cisco Small Business RV Series. Un atacante adyacente no autenticado podría ejecutar código arbitrario o causar fuga de memoria a un router afectado, provocando una condición de denegación de servicio (DoS).

CVE-2021-1362 afecta al endpoint SOAP API de distintos productos Cisco Unified Communications: Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, Cisco Unity Connection y Cisco Prime License Manager. La vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en un aparato afectado.

CVE-2021-1386 afecta al mecanismo de carga de biblioteca de enlace dinámico (DLL) en Cisco Advance Malware Protection (AMP) para los endpoints Windows Connector, ClamAV para Windows e Immunet. La vulnerabilidad podría permitir a un atacante local autenticado realizar un ataque de secuestro DLL en un sistema Windows afectado.

CVE-2021-3449 y CVE-2021-3450 son vulnerabilidades en Open SSL que también afectan a productos de Cisco. Estas vulnerabilidades fueron detalladas ya en el siguiente informe del CSIRT de Gobierno: https://www.csirt.gob.cl/noticias/alerta-ante-vulnerabilidades-en-openssl/.

El resto de las vulnerabilidades listadas en el presente informe son caracterizadas como de riesgo medio.

Productos Afectados

Cisco SD-WAN vManage Software.
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Management Interface.
Cisco Small Business RV Series.

Cisco Unified Communications Products.
Cisco Unified Communications Manager Session Management Edition.
Cisco Unified Communications Manager IM & Presence Service.
Cisco Unity Connection.
Cisco Prime License Manager.
Cisco IOS XR Software Command.
Cisco Webex Meetings para Android.
Cisco Webex Meetings.
Cisco Umbrella.
Cisco RV340, RV340W, RV345, y RV345P Dual WAN Gigabit VPN.
Cisco Unified Intelligence Center.

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-rce-q3rxHnvm
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-bypass-inject-Rbhgvfdx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-pqVYwyb
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-imm-dll-tu79hvkO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-cmdinj-vsKGherc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-andro-iac-f3UR8frB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-VObwRKWV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-inject-gbZGHP5T
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv34x-rce-8bfG2h6b
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-U2WTsUg6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-Q4PZcNzJ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-selfcare-VRWWWHgE
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-inf-disc-wCxZNjL2
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1459

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1251
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1362
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1386
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1485
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1475
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1413
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1414
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1463
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1380
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1407
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1408
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1399
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1406

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.11 23:40:56 -04'00'