Alerta de seguridad cibernética	9VSA21-00503-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2021
Última revisión	07 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 de las vulnerabilidades publicadas esta semana por Cisco.

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

Vulnerabilidades

CVE-2021-34710
CVE-2021-34735
CVE-2021-34698
CVE-2021-34748
CVE-2021-34775
CVE-2021-34776
CVE-2021-34777
CVE-2021-34778
CVE-2021-34779
CVE-2021-34780
CVE-2021-1594
CVE-2021-34788
CVE-2021-34758
CVE-2021-34766
CVE-2021-34744
CVE-2021-34757
CVE-2021-34706
CVE-2021-34702
CVE-2021-34711
CVE-2021-1534
CVE-2021-34782
CVE-2021-34742
CVE-2021-34772
CVE-2020-24586
CVE-2020-24587
CVE-2020-24588
CVE-2020-26139
CVE-2020-26140
CVE-2020-26141
CVE-2020-26142
CVE-2020-26143
CVE-2020-26144
CVE-2020-26145
CVE-2020-26146
CVE-2020-26147

Impactos

Riesgo alto

CVE-2021-34710 y CVE-2021-34735: Vulnerabilidades que afectan a Cisco ATA 190 Series Analog Telephone Adapter Software, y podrían permitir a un atacante realizar un ataque de inyección de código resultando en ejecución remota de código o una condición de denegación de servicio (DoS) en los equipos afectados.

CVE-2021-34698: Afecta a Cisco AsyncOS for Cisco Web Security Appliance (WSA) y podría permitir a un atacante remoto no autenticado agotar la memoria de sistema y provocar una condición de denegación de servicio (DoS) en el aparato afectado.

CVE-2021-34748: Vulnerabilidad en la interfaz web de administración de Cisco Intersight Virtual Appliance debida a insuficiente validación de inputs y que podría permitir a un atacante remoto autenticado realizar un ataque de inyección de comandos en un equipo afectado.

CVE-2021-34775, CVE-2021-34776, CVE-2021-34777, CVE-2021-34778, CVE-2021-34779 y CVE-2021-34780 son vulnerabilidades en la implementación del Link Layer Discovery Protocol (LLDP) para Cisco Small Business 220 Series Smart Switches. Un atacante adyacente y no autenticado podría ejecutar código, provocar un reinicio inesperado o causar corrupción de databases LLDP en un equipo afectado.

CVE-2021-1594 es una vulnerabilidad en la REST API de Cisco Identity Services Engine (ISE) que podría permitir a un atacante remoto no autenticado realizar un ataque de inyección de comandos y elevar privilegios a root.

CVE-2021-34788 es una vulnerabilidad en el mecanismo de carga de bibliotecas compartidas en Cisco AnyConnect Secure Mobility Client para Linux y Mac OS que podría permitir a un atacante local autenticado realizar un ataque de secuestro de bibliotecas en el equipo afectado si el módulo VPN Posture (HostScan) está instalado en el cliente AnyConnect.

Productos Afectados

Cisco ATA 190 Series Analog Telephone Adapter Software.
Cisco AsyncOS for Cisco Web Security Appliance (WSA).
Cisco Intersight Virtual Appliance.
Cisco Small Business 220 Series Smart Switches.
Cisco Identity Services Engine (ISE).
Cisco TelePresence Collaboration Endpoint (CE) Software y Cisco RoomOS Software.
Cisco Smart Software Manager On-Prem (SSM On-Prem).
Cisco Business 220 Series Smart Switches.
Cisco Identity Services Engine (ISE).
Cisco IP Phone software.
Cisco AsyncOS Software for Cisco Email Security Appliance (ESA).
Cisco DNA Center.
Cisco Vision Dynamic Signage Director.

Cisco Orbital.
Aironet 1532 APs, AP803 Integrated AP on IR829 Industrial Integrated Services Routers.
Aironet 1542 APs, Aironet 1810 APs, Aironet 1815 APs, Aironet 1832 APs, Aironet 1842 APs, Aironet 1852 APs, Aironet 1800i Aps.
Aironet 1552 APs, Aironet 1552H APs, Aironet 1572 APs, Aironet 1702 APs, Aironet 2702 APs, Aironet 3702 APs, IW 3702 Aps.
Aironet 1560 Series APs, Aironet 2800 Series APs, Aironet Series 3800 APs, Aironet Series 4800 APs, Catalyst IW 6300 APs, 6300 Series Embedded Services APs (ESW6300).
Catalyst 9105 APs, Catalyst 9115 APs, Catalyst 9120 APs, Integrated AP on 1100 Integrated Services Routers.
Catalyst 9117 AP.
Catalyst 9124 AP, Catalyst 9130 AP.
Meraki GR10, GR60, MR20, MR30H, MR33, MR36, MR42, MR42E, MR44, MR45, MR46, MR46E, MR52, MR53, MR53E, MR55, MR56, MR70, MR74, MR76, MR84, MR86.
Meraki MR12, MR18, MR26, MR32, MR34, MR62, MR66, MR72.
Meraki MX64W, MX65W, MX67W, MX67CW, MX68W, MX68CW, Z3, Z3C.
IP Phone 8861, IP Phone 8865 y IP Conference Phone 8832.
IP Phone 6861 y IP Phone 8861 Running Third-Party Call Control (3PCC) Software.
Wireless IP Phone 8821.
Webex Desk Series y Webex Room Series.
Webex Board Series.
Webex Wireless Phone 840 y 860.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/publicationListing.x
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wifi-faf-22epcEWu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-amp-redirect-rQ2Bu7dU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvdsd-xss-fvdj6HK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-infodisc-KyC6YncS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-sGcfsDrp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-arbfileread-NPdtE2Ow
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-disc-pNXtLhdp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-V4VSjEsX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-hardcoded-cred-MJCEXvX
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-priv-esc-5g35cdDJ

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tpce-rmos-mem-dos-rck56tT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-priv-esc-UwqPrBM3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsi2-command-inject-CGyC8y2R
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-dos-fmHdKswk
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-A4J57F3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-lib-hija-cAFB7x4q
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34710
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1594
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34711
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1534
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26139
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26141
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26142

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26145
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26146
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26147

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.08 10:09:43 -03'00'