Alerta de seguridad cibernética	9VSA21-00441-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	06 de mayo de 2021
Última revisión	06 de mayo 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 de Gobierno, comparte vulnerabilidades que afectan a distintos productos de Cisco.

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

Vulnerabilidades

CVE-2021-1497
CVE-2021-1498
CVE-2021-1275
CVE-2021-1468
CVE-2021-1505
CVE-2021-1506
CVE-2021-1508
CVE-2021-1426
CVE-2021-1427
CVE-2021-1428
CVE-2021-1429
CVE-2021-1430
CVE-2021-1496
CVE-2021-1363
CVE-2021-1365
CVE-2021-1284
CVE-2021-1421
CVE-2021-1400
CVE-2021-1401
CVE-2021-1509
CVE-2021-1510
CVE-2021-1511
CVE-2021-1513
CVE-2021-1490
CVE-2021-1438
CVE-2021-1507
CVE-2021-1486
CVE-2021-1478
CVE-2021-1532
CVE-2021-1447
CVE-2021-1234
CVE-2021-1535
CVE-2021-1514
CVE-2021-1512
CVE-2021-1515
CVE-2021-1520
CVE-2021-1521
CVE-2021-1499
CVE-2021-1516
CVE-2021-1530
CVE-2021-1519
CVE-2020-3347
CVE-2021-1493

Impactos

Las siguientes vulnerabilidades fueron calificadas de riesgo crítico por Cisco.

CVE-2021-1497 y CVE-2021-1498: Estas vulnerabilidades en Cisco HyperFlex HX podrían permitir a un atacante remoto no autenticado realizar ataques de inyección de comandos contra un aparato afectado.

CVE-2021-1275, CVE-2021-1468, CVE-2021-1505, CVE-2021-1506 y CVE-2021-1508 son vulnerabilidades en Cisco SD-WAN vManage Software que podrían permitir a un atacante remoto no autenticado ejecutar código arbitrario o ganar acceso a información sensible, o permitir a un atacante local autenticado escalar privilegios o acceso no autorizado a la aplicación.

Las siguientes vulnerabilidades fueron calificadas como de riego alto por Cisco.

CVE-2021-1426, CVE-2021-1427, CVE-2021-1428, CVE-2021-1429, CVE-2021-1430 y CVE-2021-1496: Estas vulnerabilidades en los procesos de instalación, desinstalación y mejora en Cisco AnyConnect Secure Mobility Client para Windows podrían permitir a un usuario local autenticado el secuestrar DLLo archivos ejecutables que son usados por la aplicación, y ejecutar código arbitrario en un dispositivo afectado.

CVE-2021-1284: Una vulnerabilidad en la interfaz web de mensajería de Cisco SD-WAN vManage podría permitir a un atacante no autenticado y adyacente a evadir autenticación y autorización y modificar la configuración de un sistema afectado.

CVE-2021-1363 y CVE-2021-1365: Estas vulnerabilidades en la interfaz de administración web de Cisco Unified Communications Manager IM & Presence Service podrían permitir a un atacante remoto y autenticado realizar ataques de inyección SQL en un sistema afectado.

CVE-2021-1421: Una vulnerabilidad en Cisco Enterprise NFV Infrastructure Software podría permitir a un atacante local autenticado realizar un ataque de inyección de comandos en un aparato afectado. La vulnerabilidad existe debido a una validación insuficiente del input entregado por el usuario al comando de configuración.

CVE-2021-1400 y CVE-2021-1401: Estas vulnerabilidades en la interface web de administración de algunos Cisco Small Business 100, 300 y 500 Series Wireless Access Points podrían permitir a un atacante remoto autenticado obtener información sensible de, o inyectar comandos arbitrarios en un aparato afectado.

CVE-2021-1510 y CVE-2021-1511: Estas vulnerabilidades en Cisco SD-WAN vEdge podrían permitir a un atacante ejecutar código arbitrario como usuario root o causar una condición de denegación de servicio (DoS) en el aparato afectado.

CVE-2021-1513: Esta vulnerabilidad en el proceso vDaemon de Cisco SD-Wan Software puede permitir a un atacante remoto no autenticado causar un aparato que vuelva a cargar, resultando en una condición de denegación de servicio (DoS).

CVE-2021-1493 esta vulnerabilidad en las interfaces web de Cisco Adaptative Security Appliance y Cisco Firepower Threat Defense podría permitir a un atacante remoto autenticado generar un desborde del buffer en un sistema afectado.

Productos Afectados

Cisco HyperFlex HX
Cisco AnyConnect Secure Mobility Client for Windows
Cisco SD-WAN vManage
Cisco SD-WAN vEdge
Cisco SD-WAN vBond Orchestrator Software
Cisco SD-WAN vEdge Cloud Routers
Cisco SD-WAN vEdge Routers
Cisco SD-WAN vManage Software
Cisco SD-WAN vSmart Controller Software
Cisco Unified Communications Manager IM & Presence Service
Cisco Unified Communications Manager (Unified CM)
Cisco Unified Communications Manager Session Management Edition (Unified CM SME)
Cisco Enterprise NFV Infrastructure
Cisco Small Business 100, 300 y 500 Series Wireless Access
Cisco Web Security Appliance
Cisco Wide Area Application Services
Cisco TelePresence Collaboration Endpoint (CE) Software
Cisco RoomOS Software
Cisco AsyncOS for Cisco Content Security Management Appliance (SMA)
Routers Cisco RV340, RV340W, RV345, y RV345P Dual WAN Gigabit VPN
Cisco Video Surveillance 8000 Series
Cisco Integrated Management Controller (IMC)
Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA)
Cisco Email Security Appliance (ESA)
Cisco Web Security Appliance (WSA)
Cisco BroadWorks Messaging Server Software
Cisco AnyConnect Secure Mobility Client para Windows, MacOS, y Linux anteriores al 4.10.00093
Cisco Webex Meetings Desktop App for Windows
Cisco Adaptive Security Appliance (ASA) Software
Cisco Firepower Threat Defense (FTD)

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-auth-bypass-65aYqcS2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-inj-ereCOKjR

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-cmdinj-DkFjqg2j
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-ZAfKGXhF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-xss-mVjOWchB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-waas-infdisc-Twb4EypK
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-xss-eN75jxtW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-enumeration-64eNnDKy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-dos-OO4SRYEf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-rmos-fileread-pE9sL3g
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-priv-esc-JJ8zxQsC
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmaninfdis3-OvdR6uu8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmanageinfdis-LKrFpbv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-QVszVUPy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-9VZO4gfU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcameras-dos-fc3F6LzT
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-upload-KtCK8Ugz
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bwms-xxe-uSLrZgKs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-profile-AggMUCDg
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-client-NBmqM9vt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3884
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8566
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12403
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14372
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15157
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25632
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25658
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28362
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3121
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-2021-20225
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20233
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25648
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25692
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-2020-25678

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3139
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23994
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23995
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1497
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1498
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1275
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1505
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1506
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1427
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1428
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1430
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1363
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1365
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1284
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1400
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1401
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1511
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1507
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1486
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1532
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1447
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1234
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1515
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1520
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1499
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1530
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1519
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1493

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.06 22:59:49 -04'00'