Alerta de seguridad cibernética	9VSA21-00367-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2021
Última revisión	18 de enero 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 la información entregada por Cisco, sobre vulnerabilidades que afectan a varios de sus productos.

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

Vulnerabilidad

CVE-2021-1242
CVE-2021-1311
CVE-2021-1145
CVE-2021-1224
CVE-2021-1236
CVE-2021-1258
CVE-2021-1240
CVE-2021-1127
CVE-2021-1245
CVE-2021-1246
CVE-2021-1131
CVE-2021-1267
CVE-2021-1238
CVE-2021-1239
CVE-2021-1126
CVE-2021-1130
CVE-2021-1226
CVE-2021-1143

Impacto

CVE-2021-1242 permite a un atacante remoto no autenticado manipular nombres de archivo dentro de la interfaz de mensajería de Cisco Webex Teams. Un atacante puede explotar esta vulnerabilidad compartiendo un archivo dentro de la interfaz de la aplicación, modificando la forma en que el nombre del archivo compartido se muestra dentro de la interfaz, para realizar ataques de phishing o spoofing.

CVE-2021-1311 es una vulnerabilidad en Cisco Webex Meetings Server, que podría permitir a un usuario remoto no autenticado tomar control del rol de anfitrión durante una reunión. Esta tiene lugar por una falta de protección contra ataques de fuerza bruta sobre las credenciales de anfitrión.

CVE-2021-1145: Esta vulnerabilidad en el Secure FTP (SFTP) de Cisco StarOS para los routers Cisco ASR 5000 podría permitir a un atacante remoto no autenticado leer archivos arbitrarios en un dispositivo afectado. Para explotar esta vulnerabilidad, el atacante debe tener credenciales válidas en el aparato afectado.

CVE-2021-1224: Esta vulnerabilidad en TCP Fast Open (TFO), cuando se usa junto al motor de detección Snort, podría permitir a un atacante remoto y no autenticado el evadir la política de archivos configurada para HTTP. Esto le permitiría al atacante entregar una carga maliciosa.

CVE-2021-1223: Esta vulnerabilidad en el motor de detección Snort podría permitir a un atacante remoto no autenticado evadir la política de archivos configurada para HTTP. Debido a un manejo incorrecto de un encabezado de respuesta HTTP, un atacante puede enviar paquetes HTTP a través de un aparato afectado y entregar una carga maliciosa.

CVE-2021-1236: Esta vulnerabilidad en el motor de detección de aplicaciones Snort permitiría a un atacante remoto no autenticado evadir las políticas configuradas en un sistema afectado, debido a una falla en el algoritmo de detección. Esto posibilitaría a un atacante enviar paquetes maliciosos a una red protegida a través del sistema afectado.

CVE-2021-1258: Debido a restricciones insuficiente a los permisos de archivo, esta vulnerabilidad en el componente de mejora del Cisco AnyConnect Secure Mobility Client podría permitir a un atacante local autenticado con pocos privilegios leer archivos arbitrarios en el sistema operativo (OS) de un aparato afectado, y explotar la vulnerabilidad enviando un comando diseñado desde el CLI local a la aplicación.

CVE-2021-1240: Esta es una vulnerabilidad durante el proceso de carga de DLL específicos en Cisco Proximity Desktop para Windows, que podría permitir a un atacante local autenticado cargar una biblioteca maliciosa. Para explotar esta vulnerabilidad, el atacante debe tener credenciales válidas en el sistema Windows.

CVE-2021-1127: Esta vulnerabilidad, en la interfaz de administración web de Cisco Enterprise NFV Infrastructure Software (NFVIS) podrían permitir a un atacante remoto autenticado realizar un ataque XSS contra un usuario de dicha interfaz.

CVE-2021-1245 y CVE-2021-1246: Esta vulnerabilidad, en la interfaz de administración web de Cisco Finesse podría permitir a un atacante remoto no autenticado realizar un ataque XSS y obtener información potencialmente confidencial aprovechando una falla en el mecanismo de autenticación.

CVE-2021-1131: Esta vulnerabilidad en la implementación del Cisco Discovery Protocol para las cámaras IP Cisco Video Surveillance 8000 Series podría permitir a un atacante adyacente no autenticado hacer que una cámara IP afectada se vuelva a cargar.

CVE-2021-1267: Esta vulnerabilidad en el software Cisco Firepower Management Center (FMC), debido a restricciones inadecuadas en las entidades XML, podría permitir a un usuario remoto autenticado causar un ataque de denegación de servicio (DoS) en el dispositivo afectado.

CVE-2021-1238 y CVE-2021-1239: Vulnerabilidades en la interfaz de administración web de Cisco Firepower Management Center que permitirían a un atacante remoto autenticado realizar un ataque XSS contra un usuario de dicha interfaz.

CVE-2021-1126: Una vulnerabilidad en las credenciales de servidor proxy de Cisco Firepower Center podría permitir a un atacante local autenticado ver las credenciales para un servidor proxy configurado. Un exploit exitoso podría permitir al atacante ver las credenciales que son usadas para acceder al servidor proxy.

CVE-2021-1130: Vulnerabilidad en la interfaz de administración web de Cisco DNA Center podría permitir a un atacante remoto autenticado realizar un ataque XSS contra un usuario de la interfaz o un aparato afectado. Un atacante podría explotar esta vulnerabilidad para ejecutar código arbitrario en contexto de la interfaz o acceder a información sensible.

CVE-2021-1226: Esta vulnerabilidad en un componente de Cisco Unified Communications Manager, Unified Communications Manager Session Management Edition, Unified Communications Manager IM & Presence Service, Unity Connection, Emergency Responder y Prime License Manager, podría permitir a un atacante remoto autenticado ver información sensible en un sistema afectado. La vulnerabilidad se debe al almacenamiento de ciertas credenciales no encriptadas.

CVE-2021-1143: Una vulnerabilidad en las autorizaciones API en Cisco Connected Mobile Experiences (CMX) podrían permitir a un atacante remoto autenticado enumerar qué usuarios existen en un sistema. La vulnerabilidad existe debido a la falta de chequeos de autorización para ciertas solicitudes API GET. Un exploit exitoso podría permitir a un atacante enumerar los usuarios del sistema CMX.

Productos Afectados

- CVE-2021-1242
  - Cisco Webex Teams, versiones anteriores a la 40.12.0.17293.
- CVE-2021-1311
  - Cisco Webex Meetings Server. 3.0MR3 anteriores al Parche de Seguridad 5. 4.0MR3 anteriores al Parche de Seguridad 4.

- CVE-2021-1145
    - Routers Cisco ASR 5000 Series si están ejecutando una versión de Cisco StarOS previa a la 21.19.7.
- CVE-2021-1224
    - Aparatos que usen el siguiente software
        - Software Cisco FTD anteriores al 6.6.0.
        - Software Snort Intrusion Protection System (IPS) para Cisco Unified Threat Defense (UTD) para Cisco IOS XE anteriores a la version 17.2.1r.
        - Snort de Código abierto, versiones anteriores a la 2.9.16.
- CVE-2021-1223
    - Aparatos que usen el siguiente software
        - Cisco Firepower Threat Defense (FTD) anteriores a la version 6.7.0.
        - Cisco UTD Snort IPS Engine para IOS XE, versiones anteriores a la 17.4.1.
        - Snort de código abierto, versiones anteriores a la 2.9.17.
- CVE-2021-1236
    - Aparatos que usen el siguiente software:
        - Cisco Firepower Threat Defense (FTD) anteriores a la 4ersion 6.5.0.5.
        - Cisco UTD Snort IPS Engine para IOS XE, versiones anteriores a la 17.4.1.
        - Snort de código abierto, versiones anteriores a la 2.9.14.10.
- CVE-2021-1258
    - AnyConnect Secure Mobiliy Client para Linux: versiones anteriores a la 4.9.03047.
    - AnyConnect Secure Mobiliy Client para MacOS: versiones anteriores a la 4.9.03047.
    - AnyConnect Secure Mobilty Client para Windows, versiones anteriores a la 4.9.03049.
- CVE-2021-1240
    - Cisco Proximity Desktop para Windows, versiones anteriores a la 3.1.0.
- CVE-2021-1127
    - Aparatos Cisco Enterprise NFVIS con versiones anteriores a la 4.4.1.
- CVE-2021-1245
    - Cisco Finesse, versiones anteriores a la 12.0 ES05 y 12.5 ES.05.
- CVE-2021-1246
    - Cisco Finesse, versiones anteriores a la 12.0 ES05 y 12.5 ES.05.
- CVE-2021-1131
    - Cámaras IP Cisco Video Surveillance 8000 Series con versiones de firmware anteriores al 1.0.9-8 con el Cisco Discovery Protocol activado.
- CVE-2021-1267
    - Cisco FMC, versiones anteriores a la 6.6.1.
- CVE-2021-1238
    - Cisco FMC, versiones anteriores a la 6.7.0.
- CVE-2021-1239
    - Cisco FMC, versiones anteriores a la 6.7.0.
- CVE-2021-1126
    - Cisco Firepower Management Center versiones anteriores a la 6.7.0.
- CVE-2021-1130
    - Cisco DNA Center, versiones anteriores a la 2.2.1.0.

- CVE-2021-1226
    - Unified Communications Manager (Unified CM)
    - Unified Communications Manager Session Management Edition (Unified CM SME)
    - Unified Communications Manager IM & Presence Service (Unified CM IM&P)
    - Unity Connection
    - Emergency Responder
    - Prime License Manager
- CVE-2021-1143
    - Cisco CMX, versiones 10.6.0, 10.6.1. y 10.6.2.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-7ZMcXG99

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-brutef-hostkey-FWRMxVF

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-file-read-L3RDvtey

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-app-bypass-cSBYCATq

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-fileread-PbHbgHMj

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-proximity-dll-UvW4VHPM

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-xss-smsz5Vhb

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multi-vuln-finesse-qp6gbUO2

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipcameras-dos-9zdZcUfq

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xee-DFzARDcs

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-infodisc-RJdktM6f

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-xss-HfV73cS3

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-logging-6QSWKRYz

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1242

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1311

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1145

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1224

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1236

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1258

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1240

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1127

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1245

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1246

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1131

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1267

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1238

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1239

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1126

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1130

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1226

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1143