Alerta de seguridad cibernética	9VSA21-00375-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de enero de 2021
Última revisión	26 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 en varios de sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2021-1264
CVE-2021-1257
CVE-2021-1265
CVE-2021-1138
CVE-2021-1139
CVE-2021-1140
CVE-2021-1141
CVE-2021-1142
CVE-2021-1241
CVE-2021-1273
CVE-2021-1274
CVE-2021-1278
CVE-2021-1279
CVE-2021-1302
CVE-2021-1304
CVE-2021-1305
CVE-2021-1218
CVE-2021-1259
CVE-2021-1300
CVE-2021-1301

Impacto

CVE-2021-1264 es calificado por Cisco como una vulnerabilidad crítica. Afecta a la herramienta Command Runner del Cisco DNA Center y podría permitir a un atacante remoto no autenticado realizar un ataque de inyección de comandos. La vulnerabilidad tiene lugar por una insuficiente validación de entradas por la herramienta Command Runner.

CVE-2021-1257 y CVE-2021-1265 son vulnerabilidades que afectan a Cisco DNA Center y son consideradas como de riesgo alto por el proveedor:

CVE-2021-1257 es una vulnerabilidad de falsificación de petición en sitios cruzados (CSRF) en la interfaz de administración web del Cisco Digital Network Architecture Center (Cisco DNA Center).

Un ataque CSRF fuerza al usuario a ejecutar acciones no deseadas en una aplicación web en la que se encuentra autenticado, con lo que un atacante remoto puede manipular al usuario para que ejecute acciones maliciosas sin su conocimiento o consentimiento.

CVE-2021-1265 es una vulnerabilidad en la función de archivo de configuración del Cisco Digital Network Architecture Center (Cisco DNA Center). Esta ocurre porque los archivos son guardados en texto llano, lo que puede ser recuperado por varias llamadas de la API.

Un atacante podría explotar esta vulnerabilidad a través de autenticarse en el aparato y ejecutar una serie de llamadas de la API, obteniendo las configuraciones desenmascaradas de los aparatos administrados.

CVE-2021-1138, CVE-2021-1139, CVE-2021-1140, CVE-2021-1141 y CVE-2021-1142 son calificadas por Cisco como vulnerabilidades críticas. Afectan a la interfaz de usuario (UI) del Cisco Smart Software Manager Satellite y permitirían a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente. Estas vulnerabilidades existen debido a una validación insuficiente de entradas.

Las CVE-2021-1241, CVE-2021-1273, CVE-2021-1274, CVE-2021-1278 y CVE-2021-1279 son vulnerabilidades de Denegación de Servicio que afectan a Cisco SD-WAN y que son consideradas como de riesgo alto por el proveedor.

CVE-2021-1241 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS). La vulnerabilidad existe debido a un error de límites en las funciones de túnel VPN. Un atacante remoto puede detonar una corrupción de memoria y provocar una condición DoS en el sistema objetivo.

CVE-2021-1273 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS). Esta vulnerabilidad tiene lugar por culpa del chequeo de límites en la función de túnel IPSec. Un atacante remoto puede enviar paquetes IPv4 o IPv6 especialmente diseñados, detonando una corrupción de memoria y provocar una condición DoS en el sistema objetivo.

CVE-2021-1274 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS). La vulnerabilidad existe debido a un error de desreferencia NULL pointer en vDaemon. Un atacante remoto puede enviar datos especialmente diseñados a la aplicación y realizar un ataque DoS.

CVE-2021-1278 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS). La vulnerabilidad existe por la falta de chequeos de validación para la información ingresada usada para crear enlaces simbólicos. Un usuario local puede crear un enlace simbólico a un archivo objetivo en una ruta específica y causar una condición DoS en el sistema objetivo.

CVE-2021-1279 permite a un atacante remoto realizar un ataque de denegación de servicio (DoS). La vulnerabilidad existe por la falta de chequeos de validación para la información ingresada en la funcionalidad de administración de SNMPv3. Un usuario local puede ingresar información especialmente diseñada a la aplicación y realizar un ataque DoS.

CVE-2021-1300 es una vulnerabilidad considerada de alto riesgo y que afecta a Cisco SD-WAN. Existe debido a un manejo incorrecto del tráfico IP.

Un atacante podría explotar esta vulnerabilidad al enviar tráfico IP específicamente diseñado a través de un aparato afectado, que podría causar un desbordamiento de buffer cuando el tráfico es procesado. Una explotación exitosa podría permitir al atacante ejecutar código arbitrario en el sistema operativo subyacente con privilegios de superusuario.

CVE-2021-1301 es una vulnerabilidad considerada de alto riesgo y que afecta al subsistema NETCONF de Cisco SD-WAN. Existe debido a una validación insuficiente de los datos ingresados por el usuario y leídos por el sistema durante el establecimiento de una conexión SSH. Un atacante podría explotar esta vulnerabilidad creando un archivo para leer el sistema afectado, causando un desbordamiento de buffer que podría resultar en una condición DoS en el aparato o sistema afectado.

CVE-2021-1302, CVE-2021-1304, CVE-2021-1305 afectan a Cisco SD-WAN vManage, y son consideradas de riesgo medio.

CVE-2021-1302 permite a un atacante remoto evadir chequeos de autorización. La vulnerabilidad existe debido a chequeos de autorización insuficientes en la interfaz de administración web. Un atacante remoto autenticado puede enviar una solicitud HTTP especialmente diseñada, evadir la autorización y conectar con otros inquilinos de vManage.

CVE-2021-1304 permite a un atacante remoto autenticado acceder a información sensible del sistema, debido a chequeos de autorización insuficientes en la consola SSH de la interfaz de administración web de Cisco SD-Wan vManage.

CVE-2021-1305 permite a un atacante remoto autenticado acceder a información la cual no está autorizado a ver, como logs, configuraciones e información del aparato. Esta vulnerabilidad ocurre debido a chequeos de autorización insuficientes de los privilegios de las cuentas.

CVE-2021-1218 es una vulnerabilidad de riesgo medio que afecta al Cisco Smart Software Manager Satellite. Debido a una sanitización inapropiado de los datos entregados por el usuario en la interfaz de administración web. Un atacante remoto autenticado puede crear un enlace que dirija a un dominio arbitrario.

CVE-2021-1259 es una vulnerabilidad de riesgo medio que afecta al Cisco SD-WAN vManage, y que permite a un atacante remoto realizar ataques de secuencias de directorio transversal. Un atacante remoto autenticado puede enviar una solicitud HTTP especialmente diseñada y escribir archivos arbitrarios en el sistema.

Productos afectados

CVE-2021-1264: Cisco DNA Center, versiones anteriores a la 1.3.1.0.

CVE-2021-1257 y CVE-2021-1265: Cisco DNA Center, versiones anteriores a la 2.1.1.0.

CVE-2021-1138, CVE-2021-1139, CVE-2021-1140, CVE-2021-1141 y CVE-2021-1142: Cisco Smart Software Manager Satellite, versiones anteriores a la 6.3.0. (desde la cual el producto fue renombrado como Cisco Smart Software Manager On-Prem).

CVE-2021-1241: Cisco SD-WAN (versiones 18.3.0 a 20.4.0), routers Cisco SD-WAN vEdge.

CVE-2021-1273: Cisco SD-WAN (versiones 18.3.0 a 20.4.0), Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage y Cisco SD-WAN vSmart Controller.

CVE-2021-1274: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller, y los Cisco IOS XE SD-WAN anteriores a la version 16.12.4.

CVE-2021-1278 y CVE-2021-1279: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller, y los Cisco SD-WAN versiones de la 18.3.0 a la 20.3.0.

CVE-2021-1300 y CVE-2021-1301: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller, Cisco IOS XE SD-WAN, versiones hasta la 16.12 y los Cisco SD-WAN versiones de la 18.3.0 a la 20.3.0.

CVE-2021-1302, CVE-2021-1304 y CVE-2021-1305: Cisco SD-WAN vManage, versiones de la 18.3 a la 20.4.0.

CVE-2021-1218: Cisco Smart Software Manager Satellite: 5.0

CVE-2021-1259: Cisco SD-WAN vManage, versiones anteriores a la 18.2.0.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-multici-pgG5WM5A

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-csrf-dC83cMcV

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnacid-OfeeRjcn

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-bufovulns-B5NrSHbj

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1264

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1257

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1265

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1138

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1139

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1140

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1141

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1142

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1241

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1273

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1274

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1278

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1279

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1302

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1304

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1305

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1218

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1259

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1300

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1301