Alerta de seguridad informática	9VSA-00031-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2019
Última revisión	8 de agosto de 2019

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 referente a vulnerabilidades que afectan a varios de sus productos y sus actualizaciones.

Vulnerabilidad

CVE-2019-1912
CVE-2019-1913
CVE-2019-1914
CVE-2019-1941
CVE-2019-1944
CVE-2019-1945
CVE-2019-1955
CVE-2019-1949
CVE-2019-1957
CVE-2019-1970
CVE-2019-1958
CVE-2019-1952
CVE-2019-1971
CVE-2019-1961
CVE-2019-1972
CVE-2019-1953
CVE-2019-1959
CVE-2019-1960
CVE-2019-1973
CVE-2019-1946
CVE-2019-1951
CVE-2019-1956
CVE-2019-1954
CVE-2019-1934
CVE-2019-1910
CVE-2019-1918
CVE-2019-1895
CVE-2019-1924
CVE-2019-1925
CVE-2019-1926
CVE-2019-1927
CVE-2019-1928
CVE-2019-1929

Impacto

CVE-2019-1912

Una vulnerabilidad en la interfaz de administración web de Cisco Small Business 220 Series Smart Switches podría permitir que un atacante remoto no autenticado cargue archivos arbitrarios.

CVE-2019-1913

Múltiples vulnerabilidades en la interfaz de administración web de Cisco Small Business 220 Series Smart Switches podrían permitir que un atacante remoto no autenticado desborde un búfer, lo que luego permite la ejecución de código arbitrario con privilegios de root en el sistema operativo subyacente.

CVE-2019-1914

Una vulnerabilidad en la interfaz de administración web de Cisco Small Business 220 Series Smart Switches podría permitir que un atacante remoto autenticado realice un ataque de inyección de comando.

CVE-2019-1941

Una vulnerabilidad en la interfaz de administración basada en la web de Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto no autenticado realice un ataque de cross-site scripting (XSS) contra un usuario de la interfaz de administración web de un dispositivo afectado

CVE-2019-1944

Una vulnerabilidad en la funcionalidad de túnel inteligente de Cisco ASA podría permitir a un atacante local autenticado elevar los privilegios al usuario *root*. Esta escalada de privilegios ocurre en un dispositivo cliente que intenta establecer una conexión de túnel inteligente con Cisco ASA. La escalada no se produce en el propio ASA.

CVE-2019-1945

Una vulnerabilidad en la funcionalidad de túnel inteligente de Cisco ASA podría permitir que un atacante local autenticado sobrescriba archivos de sistema específicos, que luego podrían cargarse y ejecutarse durante el establecimiento de la conexión de túnel inteligente. El atacante podría realizar estas acciones en el dispositivo del cliente que intenta establecer la conexión de túnel inteligente con el ASA de Cisco y no en el propio ASA.

CVE-2019-1955

Una vulnerabilidad en la funcionalidad Sender Policy Framework (SPF) de Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) podría permitir que un atacante remoto no autenticado omita los filtros de usuario configurados en el dispositivo. Una explotación exitosa podría permitir al atacante evitar los filtros de encabezado que están configurados para el dispositivo afectado, lo que podría permitir que el contenido malicioso pase a través del dispositivo.

CVE-2019-1949

Una vulnerabilidad en la interfaz de administración basada en web de Cisco Firepower Management Center podría permitir que un atacante remoto autenticado realice un ataque de "cross-site scripting" (XSS) contra un usuario de la interfaz de administración basada en web de un sistema afectado.

CVE-2019-1957

Una vulnerabilidad en la interfaz web de Cisco IoT Field Network Director podría permitir que un atacante remoto no autenticado desencadene un uso elevado de la CPU, lo que provocaría una condición de denegación de servicio (DoS) en un dispositivo afectado.

CVE-2019-1970

Una vulnerabilidad en el motor de inspección de protocolo Secure Sockets Layer (SSL) / Transport Layer Security (TLS) del software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado omita las políticas de archivo configuradas en un sistema afectado. Una explotación exitosa podría permitir al atacante eludir las políticas de archivos configuradas y entregar una carga maliciosa a la red protegida.

CVE-2019-1958

Una vulnerabilidad en la interfaz de administración basada en la web del software Cisco HyperFlex podría permitir que un atacante remoto no autenticado realice un ataque de falsificación de solicitud entre sitios (CSRF) en un sistema afectado. La vulnerabilidad se debe a protecciones CSRF insuficientes para la interfaz de usuario web en un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que siga un enlace malicioso. Una explotación exitosa podría permitir al atacante realizar acciones arbitrarias con el nivel de privilegio del usuario afectado

CVE-2019-1952

Una vulnerabilidad en la CLI de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante local autenticado sobrescriba o lea archivos arbitrarios. El atacante necesitaría credenciales válidas de nivel de privilegio de administrador. Una explotación exitosa podría permitir al atacante sobrescribir o leer archivos arbitrarios en un dispositivo afectado.

CVE-2019-1971

Una vulnerabilidad en el portal web de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante remoto no autenticado realice un ataque de inyección de comandos y ejecute comandos arbitrarios con privilegios de root. La vulnerabilidad se debe a una validación de entrada insuficiente por parte del marco del portal web. Un atacante podría aprovechar esta vulnerabilidad al proporcionar información maliciosa durante la autenticación del portal web. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios con privilegios de root en el sistema operativo subyacente.

CVE-2019-1961

Una vulnerabilidad en el software de infraestructura de Cisco Enterprise NFV (NFVIS) podría permitir que un atacante remoto autenticado lea archivos arbitrarios en el sistema operativo (SO) subyacente de un dispositivo afectado. La vulnerabilidad se debe a la validación de entrada incorrecta de los paquetes tar cargados a través del portal web al repositorio de imágenes. Un atacante podría aprovechar esta vulnerabilidad al cargar un paquete tar diseñado y ver las entradas de registro que se generan. Una explotación exitosa podría permitir al atacante leer archivos arbitrarios en el sistema operativo subyacente.

CVE-2019-1972

Una vulnerabilidad en el CLI restringido de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante local autenticado con credenciales válidas de nivel de administrador eleve los privilegios y ejecute comandos arbitrarios en el sistema operativo subyacente como root. Un atacante podría explotar esta vulnerabilidad al aprovechar las restricciones insuficientes durante la ejecución de un comando afectado. Una explotación exitosa podría permitir al atacante elevar los privilegios y ejecutar comandos arbitrarios en el sistema operativo subyacente como root.

CVE-2019-1953

Una vulnerabilidad en el portal web de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante remoto autenticado vea una contraseña en texto claro. La vulnerabilidad se debe al inicio de sesión incorrecto de la contraseña de administrador cuando un usuario se ve obligado a modificar la contraseña predeterminada al iniciar sesión en el portal web por primera vez. Los cambios de contraseña posteriores no se registran y otras cuentas no se ven afectadas. Un atacante podría aprovechar esta vulnerabilidad al ver la contraseña de texto sin cifrar del administrador y usarla para acceder al sistema afectado. El atacante necesitaría una cuenta de usuario válida para aprovechar esta vulnerabilidad.

CVE-2019-1959

Una vulnerabilidad en Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante local autenticado lea archivos arbitrarios en el sistema operativo (SO) subyacente de un dispositivo afectado. La vulnerabilidad se debe a la validación de entrada incorrecta de los argumentos utilizados con un comando CLI vulnerable. Un atacante podría aprovechar esta vulnerabilidad mediante el uso de un argumento diseñado durante la ejecución de un comando afectado. Una explotación exitosa podría permitir al atacante leer archivos arbitrarios en el sistema operativo subyacente.

CVE-2019-1960

Una vulnerabilidad en "Cisco Enterprise NFV Infrastructure Software (NFVIS)" podría permitir que un atacante local autenticado lea archivos arbitrarios en el sistema operativo (SO) subyacente de un dispositivo afectado. La vulnerabilidad se debe a la validación de entrada incorrecta de los argumentos utilizados con un comando CLI vulnerable. Un atacante podría aprovechar esta vulnerabilidad mediante el uso de un argumento diseñado durante la ejecución de un comando afectado. Una explotación exitosa podría permitir al atacante leer archivos arbitrarios en el sistema operativo subyacente.

CVE-2019-1973

Una vulnerabilidad en el framework del portal web de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante remoto autenticado realice un ataque cross-site scriptong (XSS) contra un usuario de la interfaz web. La vulnerabilidad se debe a una validación de entrada incorrecta del contenido del archivo de registro almacenado en el dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad modificando un archivo de registro con código malicioso y haciendo que un usuario vea el archivo de registro modificado. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.

CVE-2019-1946

Una vulnerabilidad en la interfaz web de administración de "Cisco Enterprise NFV Infrastructure Software (NFVIS)" podría permitir que un atacante remoto no autenticado omita la autenticación y obtenga acceso limitado a la interfaz de administración basada en la web. La vulnerabilidad se debe a una implementación incorrecta de la autenticación en la interfaz de administración basada en la web. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud de autenticación diseñada a la interfaz de administración basada en la web en un sistema afectado. Un exploit exitoso podría permitir al atacante ver detalles de configuración limitados y potencialmente cargar una imagen de máquina virtual.

CVE-2019-1951

Una vulnerabilidad en las características de filtrado de paquetes de la solución SD-WAN de Cisco podría permitir que un atacante remoto no autenticado omita los filtros de tráfico L3 y L4. La vulnerabilidad se debe a condiciones de filtrado de tráfico inadecuadas en un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad creando un paquete TCP malicioso con características específicas y enviándolo a un dispositivo de destino. Una explotación exitosa podría permitir al atacante evitar los filtros de tráfico L3 y L4 e inyectar un paquete arbitrario en la red.

CVE-2019-1956

Una vulnerabilidad en la interfaz web de Cisco SPA112 2-Port Phone Adapter podría permitir que un atacante remoto autenticado realice un ataque de cross-site scripting (XSS) contra otro usuario del dispositivo. La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario por la interfaz basada en la web del dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad insertando código malicioso en uno de los campos de configuración. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador.

CVE-2019-1954

Una vulnerabilidad en la interfaz web de administración de Cisco Webex Meetings Server Software podría permitir que un atacante remoto no autenticado redirija a un usuario a una página web no deseada. La vulnerabilidad se debe a una validación de entrada incorrecta de los parámetros de URL en una solicitud HTTP que se envía a un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad al crear una solicitud HTTP que podría hacer que la aplicación web redirija la solicitud a una URL maliciosa especificada.

CVE-2019-1934

Una vulnerabilidad en la interfaz web de administración de Cisco Adaptive Security Appliance (ASA) Software podría permitir a un atacante remoto autenticado elevar los privilegios y ejecutar funciones administrativas en un dispositivo afectado. La vulnerabilidad se debe a una validación de autorización insuficiente. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión en un dispositivo afectado como un usuario con pocos privilegios y luego enviando solicitudes HTTPS específicas para ejecutar funciones administrativas utilizando la información recuperada durante el inicio de sesión inicial.

CVE-2019-1910

Una vulnerabilidad en la implementación de la funcionalidad del protocolo IS – IS (Intermediate System to intermediate System) en Cisco IOS XR Software podría permitir que un atacante no autenticado que se encuentre en la misma área IS – IS cause una denegación de servicio (DoS). La vulnerabilidad se debe al procesamiento incorrecto de las unidades de datos de protocolo de estado de enlace (PDU) IS – IS diseñadas. Un atacante podría aprovechar esta vulnerabilidad enviando una

PDU de estado de enlace diseñada a un sistema afectado para su procesamiento. Una explotación exitosa podría permitir que el atacante provoque que todos los enrutadores dentro del área IS – IS reinicien inesperadamente el proceso IS – IS, resultando en una condición DoS.

CVE-2019-1918

Una vulnerabilidad en la implementación de la funcionalidad del protocolo IS – IS (Intermediate System to intermediate System) en Cisco IOS XR Software podría permitir que un atacante no autenticado que se encuentre en la misma área IS – IS cause una denegación de servicio (DoS). Una explotación exitosa podría permitir al atacante causar cálculos incorrectos utilizados en los grupos de enlace de riesgo compartido remoto ponderado (SRLG) o en el Algoritmo flexible IGP. También podría causar trazas a los registros o potencialmente causar que el dispositivo receptor bloquee el proceso IS-IS, lo que resulta en una condición DoS.

CVE-2019-1895

Una vulnerabilidad en la implementación de la consola de Virtual Network Computing (VNC) de Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante remoto no autenticado acceda a la sesión de la consola VNC de un usuario administrativo en un dispositivo afectado. La vulnerabilidad se debe a un mecanismo de autenticación insuficiente para establecer una sesión VNC. Un atacante podría aprovechar esta vulnerabilidad interceptando una solicitud de sesión de VNC del administrador antes de iniciar sesión. Un exploit exitoso podría permitir al atacante mirar la sesión de la consola del administrador o interactuar con ella, permitiendo el acceso del administrador al dispositivo afectado.

CVE-2019-1924 ~ CVE-2019-1929

Múltiples vulnerabilidades en Cisco Webex Network Recording Player para Microsoft Windows y Cisco Webex Player para Microsoft Windows podrían permitir que un atacante ejecute código arbitrario en un sistema afectado. Las vulnerabilidades existen porque el software afectado valida incorrectamente los archivos de formato de grabación avanzado (ARF) y de formato de grabación Webex (WRF). Un atacante podría aprovechar estas vulnerabilidades enviando a un usuario un archivo ARF o WRF malicioso a través de un enlace o archivo adjunto de correo electrónico y persuadiendo al usuario para que abra el archivo con el software afectado en el sistema local. Una explotación exitosa podría permitir al atacante ejecutar código arbitrario en el sistema afectado con los privilegios del usuario objetivo.

Productos Afectados

- Cisco Small Business 220 Series Smart Switches con versión firmware anterior a 1.1.4.4
- Cisco ISE versión de software anterior a 2,4,0 Patch 9
- Cisco ASA Software, desde las versiones 9.4 a 9.12
- Cisco AsyncOS Software for Cisco ESA versiones anteriores a 4.0MR1.
- Cisco Firepower Management Center versiones anteriores a 6.4.0
- Cisco IoT Field Network Director versiones anteriores a 4.4.2-11
- Cisco FTD Software versiones anteriores a 6.4.0 y con políticas de archivos configuradas
- Cisco HyperFlex Software versiones anteriores a 4.0(2a).
- Cisco Enterprise NFVIS
- Cisco SD-WAN Solution versión 19.1.0 y anteriores.
    - vBond Orchestrator Software
    - vEdge 100 Series Routers
    - vEdge 1000 Series Routers
    - vEdge 2000 Series Routers
    - vEdge 5000 Series Routers
    - vEdge Cloud Router Platform
    - vManage Network Management Software
    - vSmart Controller Software
- Cisco Webex Meetings Server Software versiones anteriores a 4.0(1).
- Cisco IOS XR Software versiones anteriores a 6.6.3 y con el protocolo IS-IS configurado.
- Cisco Webex Business Suite sites versiones anteriores a WBS 39.5.5
- Cisco Webex Meetings Online versiones anterior a 1.3.43
- Cisco Webex Meetings Server versiones anteriores a 2.8MR3Patch3, 3.0MR2Patch4, 4.0, o 4.0MR1

Mitigación

Instalar las actualizaciones liberadas por el fabricante directamente de su página web.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-auth_bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190806-sb220-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190717-ise-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-asa-multi

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-esm-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-fmc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-fnd-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-ftd-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-hypflex-csrf
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-cli-path
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-commandinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-fileread
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-privescal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-pwrecov
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-read
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfv-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfvis-authbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-sd-wan-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-spa112-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-wms-oredirect
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-asa-privescala
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-iosxr-isis-dos-1910
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-nfvis-vnc-authbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-webex-player

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.08 13:11:14 -04'00'