Alerta de seguridad informática	9VSA20-00162-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de marzo de 2020
Última revisión	23 de marzo de 2020

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 diversas vulnerabilidades que afectan a sus productos. El presente informe incluye las respectivas medidas de mitigación.

VULNERABILIDADES

CVE-2020-3167
CVE-2020-3171
CVE-2020-3172
CVE-2020-3166
CVE-2019-16012
CVE-2019-16010
CVE-2020-3264
CVE-2020-3266
CVE-2020-3265

CVE-20-3167

Impacto

Una vulnerabilidad en la interfaz de línea de comandos (CLI) del software Cisco FXOS y del software Cisco UCS Manager podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el sistema operativo (SO) subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría explotar esta vulnerabilidad al incluir argumentos diseñados para comandos específicos. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario actualmente conectado para todas las plataformas afectadas, excluyendo las interconexiones Fabric Cisco UCS 6400 Series. En las interconexiones Fabric de Cisco UCS 6400 Series, los comandos inyectados se ejecutan con privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FXOS o del software Cisco UCS Manager:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-ucs-cmdinj

CVE-20-3171

Impacto

Una vulnerabilidad en la interfaz de línea de comandos (CLI) de administración local (local-mgmt) del software Cisco FXOS y del software Cisco UCS Manager podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el sistema operativo (SO) subyacente de un dispositivo afectado.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría explotar esta vulnerabilidad al incluir argumentos diseñados para comandos específicos. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario actualmente conectado para todas las plataformas afectadas, excluyendo las interconexiones Fabric Cisco UCS 6400 Series. En las interconexiones Fabric de Cisco UCS 6400 Series, los comandos inyectados se ejecutan con privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FXOS o del software Cisco UCS Manager:

- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-ucs-cli-cmdinj

CVE-20-3172

Impacto

Una vulnerabilidad en la función de Cisco Discovery Protocol del software Cisco FXOS y el software Cisco NX-OS podría permitir que un atacante adyacente no autenticado ejecute código arbitrario como root o cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

La vulnerabilidad existe debido a los encabezados de paquetes de Cisco Discovery Protocol insuficientemente validados. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete de Cisco Discovery Protocol diseñado a un dispositivo afectado adyacente a la Capa 2. Una explotación exitosa podría permitir al atacante causar un desbordamiento del búfer que podría permitirle ejecutar código arbitrario como root o causar una condición DoS en el dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FXOS o del software Cisco NX-OS y si están configurados para usar el Protocolo de descubrimiento de Cisco:

- Firepower 4100 Series
- Firepower 9300 Security Appliances
- MDS 9000 Series Multilayer Switches
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in standalone NX-OS mode
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-nxos-cdp

CVE-20-3166

Impacto

Una vulnerabilidad en la CLI del software Cisco FXOS podría permitir que un atacante local autenticado lea o escriba archivos arbitrarios en el sistema operativo (SO) subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad al incluir argumentos diseñados para un comando CLI específico. Una explotación exitosa podría permitir al atacante leer o escribir en archivos arbitrarios en el sistema operativo subyacente.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban una versión vulnerable del software Cisco FXOS:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-cli-file

CVE-20-16012

Impacto

Una vulnerabilidad en la interfaz web del software vManage de la solución SD-WAN de Cisco podría permitir que un atacante remoto autenticado realice ataques de inyección SQL en un sistema afectado.

La vulnerabilidad existe porque la interfaz de usuario web valida incorrectamente los valores de SQL. Un atacante podría aprovechar esta vulnerabilidad autenticándose en la aplicación y enviando consultas SQL maliciosas a un sistema afectado. Una explotación exitosa podría permitir al atacante modificar valores o devolver valores de la base de datos subyacente, así como del sistema operativo.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de software vManage de la solución SD-WAN de Cisco anteriores a la versión 19.2.2.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200318-vmanage-cypher-inject

CVE-20-16010

Impacto

Una vulnerabilidad en la interfaz web del software Cisco SD-WAN vManage podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz de administración basada en web del software vManage. La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario en la interfaz de administración web. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que haga clic en un enlace diseñado. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz o acceder a información confidencial basada en el navegador.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco vManage anteriores a la versión 19.2.2.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200318-vmanage-xss

CVE-20-3264

Impacto

Una vulnerabilidad en el software de la Solución SD-WAN de Cisco podría permitir que un atacante local autenticado cause un desbordamiento del búfer en un dispositivo afectado.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico diseñado a un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener acceso a información a la que no está autorizado y ejecutar cambios en el sistema que no está autorizado a realizar.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de software de la Solución SD-WAN de Cisco anterior a la Versión 19.2.2:

- 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

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanbo-QKcABnS2

CVE-20-3266

Impacto

Una vulnerabilidad en la interfáz de linea de comandos (CLI) del software Cisco SD-WAN Solution podría permitir que un atacante local autenticado inyecte comandos arbitrarios que se ejecutan con privilegios de root.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría explotar esta vulnerabilidad autenticándose en el dispositivo y enviando datos diseñados a la utilidad CLI. El atacante debe estar autenticado para acceder a la utilidad CLI. Una explotación exitosa podría permitir al atacante ejecutar comandos con privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de software de la Solución SD-WAN de Cisco anterior a la Versión 19.2.2:

- 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 System
- vSmart Controller Software

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwclici-cvrQpH9v

CVE-20-3265

Impacto

Una vulnerabilidad en el software de soluciones de Cisco SD-WAN podría permitir a un atacante local autenticado elevar los privilegios de root en el sistema operativo subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud diseñada a un sistema afectado. Una explotación exitosa podría permitir al atacante obtener privilegios de nivel raíz.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de software de la Solución SD-WAN de Cisco anterior a la Versión 19.2.2:

- 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 System
- vSmart Controller Software

Más detalles se pueden encontrar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwpresc-ySJGvE9