Alerta de seguridad informática	9VSA20-00137-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de febrero de 2020
Última revisión	07 de febrero 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 información obtenida de Cisco, referente a diversas vulnerabilidades que afectan a sus productos. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2019-15253
CVE-2019-15972
CVE-2019-15993
CVE-2020-3110
CVE-2020-3111
CVE-2020-3117
CVE-2020-3118
CVE-2020-3119
CVE-2020-3120
CVE-2020-3147
CVE-2020-3149

Impacto

CVE-2019-15993

Una vulnerabilidad clasificada como alta en la interfaz de usuario web de los Cisco Small Business Switches podría permitir que un atacante remoto no autenticado acceda a información confidencial del dispositivo. La vulnerabilidad existe porque el software carece de controles de autenticación adecuados a la información accesible desde la interfaz de usuario web. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP maliciosa a la interfaz de usuario web de un dispositivo afectado. Una explotación exitosa podría permitir al atacante acceder a información confidencial del dispositivo, que incluye archivos de configuración.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de firmware anterior a 2.5.0.92:

- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de firmware anterior a 1.4.11.4:

- 200 Series Smart Switches
- 300 Series Managed Switches
- 500 Series Stackable Managed Switches

Impacto

CVE-2020-3147

Una vulnerabilidad clasificada como alta en la interfaz web de los Cisco Small Business Switches podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado. La vulnerabilidad se debe a una validación incorrecta de las solicitudes enviadas a la interfaz web. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud maliciosa a la interfaz web de un dispositivo afectado. Una explotación exitosa podría permitir al atacante provocar una recarga inesperada del dispositivo, lo que provocaría una condición DoS.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de firmware anterior a 1.3.7.18:

- 250 Series Smart Switches
- 350 Series Managed Switches
- 350X Series Stackable Managed Switches
- 550X Series Stackable Managed Switches

Impacto

CVE-2020-3117

Una vulnerabilidad clasificada como media en el API Framwork de Cisco AsyncOS para Cisco Web Security Appliance (WSA) y Cisco Content Security Management Appliance (SMA) podría permitir que un atacante remoto no autenticado inyecte encabezados HTTP diseñados en la respuesta del servidor web. La vulnerabilidad se debe a una validación insuficiente de la entrada del usuario. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario para que acceda a una URL diseñada y reciba una respuesta HTTP maliciosa. Una explotación exitosa podría permitir al atacante inyectar encabezados HTTP arbitrarios en respuestas HTTP válidas enviadas al navegador de un usuario.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones 12.0.1-268 y 11.8.0-382 de Cisco WSA. Ninguna versión anterior a WSA 11.8 se ve afectada por esta vulnerabilidad. En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco SMA anteriores a la versión 13.0.0-187.

Impacto

CVE-2019-15253

Una vulnerabilidad clasificada como media en la interfaz de administración web de Cisco Digital Network Architecture (DNA) Center podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz de administración web de un dispositivo afectado. La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario por la interfaz de administración web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario 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 afectada o acceder a información confidencial basada en el navegador. Para aprovechar esta vulnerabilidad, el atacante necesita credenciales de administrador.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco DNA Center Software anteriores a 1.3.0.6 y 1.3.1.4.

Impacto

CVE-2020-3149

Una vulnerabilidad clasificada como media en la interfaz de administración web del software Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) almacenado en un dispositivo afectado. Esta vulnerabilidad se debe a una validación de entrada insuficiente por parte de la interfaz de administración web. Un atacante podría aprovechar esta vulnerabilidad al proporcionar datos maliciosos a un campo específico dentro de la interfaz. 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.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco ISE Software anteriores a la versión 2.7.0.

Impacto

CVE-2020-3118

Una vulnerabilidad clasificada como alta en la implementación de Cisco Discovery Protocol para el software Cisco IOS XR podría permitir que un atacante adyacente no autenticado ejecute código arbitrario o cause una recarga en un dispositivo afectado. La vulnerabilidad se debe a la validación incorrecta de la entrada de cadena de ciertos campos en los mensajes de Cisco Discovery Protocol. Un atacante podría explotar esta vulnerabilidad enviando un paquete malicioso de Cisco Discovery Protocol a un dispositivo afectado. Una explotación exitosa podría permitir al atacante causar un desbordamiento de la pila, lo que podría permitir al atacante ejecutar código arbitrario con privilegios administrativos en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si tienen Cisco Discovery Protocol habilitado tanto globalmente como al menos en la interfaz y si están ejecutando una versión vulnerable del software Cisco IOS XR (32 bits o 64 bits):

- ASR 9000 Series Aggregation Services Routers
- Carrier Routing System (CRS)
- IOS XRv 9000 Router
- Network Convergence System (NCS) 540 Series Routers
- Network Convergence System (NCS) 560 Series Routers
- Network Convergence System (NCS) 1000 Series Routers
- Network Convergence System (NCS) 5000 Series Routers
- Network Convergence System (NCS) 5500 Series Routers
- Network Convergence System (NCS) 6000 Series Routers

Impacto

CVE-2020-3110

Una vulnerabilidad clasificada como alta en la implementación de Cisco Discovery Protocol para las cámaras IP de Cisco Video Surveillance serie 8000 podría permitir que un atacante adyacente no autenticado ejecute código de forma remota o provoque una recarga de una cámara IP afectada. La vulnerabilidad se debe a que faltan verificaciones al procesar los mensajes de Cisco Discovery Protocol. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete malicioso de Cisco Discovery Protocol a la cámara IP objetivo. Una explotación exitosa podría permitir al atacante exponer la cámara IP afectada para la ejecución remota de código o hacer que se vuelva a cargar inesperadamente, lo que provocaría una condición de denegación de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta a las cámaras IP de Cisco Video Surveillance serie 8000 con el Cisco Discovery Protocol activado cuando ejecutan una versión de firmware anterior a la 1.0.7.

Impacto

CVE-2020-3111

Una vulnerabilidad clasificada como alta en la implementación de Cisco Discovery Protocol para el teléfono IP de Cisco podría permitir que un atacante adyacente no autenticado ejecute código de forma remota con privilegios de root o provoque una recarga de un teléfono IP afectado. La vulnerabilidad se debe a que faltan verificaciones al procesar los mensajes de Cisco Discovery Protocol. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete de Cisco Discovery Protocol diseñado al teléfono IP objetivo. Una explotación exitosa podría permitir al atacante ejecutar código de forma remota con privilegios de root o provocar una recarga de un teléfono IP afectado, lo que provocaría una condición de denegación de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta a los siguientes teléfonos IP de Cisco con Cisco Discovery Protocol habilitado y que ejecutan una versión de firmware vulnerable:

- IP Conference Phone 7832
- IP Conference Phone 7832 with Multiplatform Firmware
- IP Conference Phone 8832
- IP Conference Phone 8832 with Multiplatform Firmware
- IP Phone 6821, 6841, 6851, 6861, 6871 with Multiplatform Firmware
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones
- IP Phone 7811, 7821, 7841, 7861 Desktop Phones with Multiplatform Firmware
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones
- IP Phone 8811, 8841, 8851, 8861, 8845, 8865 Desktop Phones with Multiplatform Firmware
- Unified IP Conference Phone 8831
- Unified IP Conference Phone 8831 for Third-Party Call Control
- Wireless IP Phone 8821, 8821-EX

Nota: Cisco Discovery Protocol está habilitado de manera predeterminada en la mayoría de los modelos de teléfonos IP.

Impacto

CVE-2019-15972

Una vulnerabilidad clasificada como media en la interfaz de administración web de Cisco Unified Communications Manager podría permitir que un atacante remoto autenticado realice ataques de inyección SQL en un sistema afectado. La vulnerabilidad existe porque la interfaz de administración basada en web valida incorrectamente los valores de SQL. Un atacante podría aprovechar esta vulnerabilidad autenticándose en la aplicación y enviando solicitudes maliciosas a un sistema afectado. Una explotación exitosa podría permitir al atacante modificar valores o devolver valores de la base de datos subyacente.

Productos Afectados

En el momento de la publicación, Cisco Unified Communications Manager versiones 12.5 (1) SU2 y 11.5 (1) SU7.

Impacto

CVE-2020-3120

Una vulnerabilidad clasificada como alta en la implementación del Cisco Discovery Protocol para el software Cisco FXOS, el software Cisco IOS XR y el software Cisco NX-OS podría permitir que un atacante adyacente no autenticado provoque una recarga de un dispositivo afectado, lo que provocaría una condición de denegación de servicio (DoS). La vulnerabilidad se debe a una falta de verificación cuando el software afectado procesa los mensajes del Cisco Discovery Protocol. Un atacante podría explotar esta vulnerabilidad enviando un paquete malicioso de Cisco Discovery Protocol a un dispositivo afectado. Una explotación exitosa podría permitir que el atacante agote la memoria del sistema, haciendo que el dispositivo se recargue.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si tienen Cisco Discovery Protocol habilitado tanto a nivel global como en al menos una interfaz y si están ejecutando una versión vulnerable de Cisco FXOS, IOS XR (32 bits o 64 bits) o NX-OS Software:

- ASR 9000 Series Aggregation Services Routers
- Carrier Routing System (CRS)
- Firepower 4100 Series
- Firepower 9300 Security Appliances
- IOS XRv 9000 Router
- MDS 9000 Series Multilayer Switches
- Network Convergence System (NCS) 540 Series Routers
- Network Convergence System (NCS) 560 Series Routers
- Network Convergence System (NCS) 1000 Series
- Network Convergence System (NCS) 5000 Series
- Network Convergence System (NCS) 5500 Series
- Network Convergence System (NCS) 6000 Series
- 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
- UCS 6400 Series Fabric Interconnects

Esta vulnerabilidad también afecta a los enrutadores de caja blanca de terceros si tienen habilitado Cisco Discovery Protocol a nivel mundial y en al menos una interfaz y si están ejecutando una versión vulnerable del software Cisco IOS XR.

Impacto

CVE-2020-3119

Una vulnerabilidad clasificada como alta en la implementación de Cisco Discovery Protocol para el software Cisco NX-OS podría permitir que un atacante adyacente no autenticado ejecute código arbitrario o cause una recarga en un dispositivo afectado. La vulnerabilidad existe porque el analizador de Cisco Discovery Protocol no valida correctamente la entrada para ciertos campos en un mensaje de Cisco Discovery Protocol. Un atacante podría explotar esta vulnerabilidad enviando un paquete malicioso de Cisco Discovery Protocol a un dispositivo afectado. Una explotación exitosa podría permitir al atacante causar un desbordamiento de la pila, lo que podría permitir al atacante ejecutar código arbitrario con privilegios administrativos en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si tienen habilitado Cisco Discovery Protocol tanto a nivel global como en al menos una interfaz y si están ejecutando una versión vulnerable del software Cisco NX-OS:

- Nexus 3000 Series Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 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
- UCS 6400 Series Fabric Interconnects

Mitigación

Se deben aplicar las actualizaciones publicadas por el fabricante.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200129-smlbus-switch-disclos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smlbus-switch-dos-R6VquS2u
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-wsa-sma-header-inject
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190205-dnac-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-DxJsRWRx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-ipcameras-rce-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-voip-phones-rce-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-cucm-sql
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-nxos-cdp-rce

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.09 21:39:57 -03'00'