BAFING

Fecha:		**28/08/2024**		
Detalle reportado:		**Boletín – Vulnerabilidades en productos de Cisco**		
Caso de uso:		**CUS_GRL_04_Boletines**		
Severidad:	⚠	Riesgo grave, requiere atención de alta prioridad.	X	
	⚠	Riesgo intermedio, validación de problemas menores.		
	⚠	No hay problemas graves. Alerta informativa.		
Estado:		**Alertado**		

Descripción

Boletín – Vulnerabilidades en productos de Cisco

CISCO NX-OS

CVE-2024-20446: Vulnerabilidad en Cisco NX-OS permite ataque de denegación de servicio**. - (ALTA)**

Se detectó una vulnerabilidad de manejo inadecuado de campos específicos en un mensaje RELAY-REPLY de DHCPv6 en el software Cisco NX-OS, el cual permite que un atacante remoto no autenticado envíe un paquete DHCPv6 específicamente diseñado a cualquier dirección IPv6, para provocar que el proceso “dhcp_snoop” se bloquee y genere una condición de denegación de servicio.

Los switches Cisco Nexus 3000 Series, Cisco Nexus 7000 Series Y Cisco Nexus 9000 Series se encuentran afectados si están ejecutando una versión vulnerable de Cisco NX-OS, y cuentan con el agente de retransmisión DHCPv6 habilitado, o presentan al menos una dirección IPv6 configurada en los dispositivos afectados.

Productos afectados:

- Cisco NX-OS versión 8.2(11)
- Cisco NX-OS versión 9.3(9)
- Cisco NX-OS versión 10.2(1) y 10.2(1q)

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco NX-OS. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn

CVE-2024-20411: Vulnerabilidad en Cisco NX-OS permite ejecución de código arbitrario**. - (MEDIA)**

Cisco NX-OS presenta una vulnerabilidad de restricciones de seguridad insuficientes durante la ejecución de comandos desde el shell Bash. Un atacante local autenticado, con privilegios para acceder al shell Bash, puede aprovechar la vulnerabilidad al ejecutar un comando específico creado en el sistema operativo subyacente, y permitir la ejecución de código arbitrario con los privilegios de "root".

CVE-2024-20413: Vulnerabilidad en Cisco NX-OS permite escalación de privilegios**. - (MEDIA)**

Una vulnerabilidad de restricciones de seguridad insuficientes al ejecutar argumentos de la aplicación desde el shell Bash permite que un atacante local autenticado, con privilegios para acceder al shell Bash, ejecute un comando específico creado en el sistema operativo subyacente, para que de esta manera pueda crear nuevos usuarios con los privilegios de "network-admin".

Los switches Nexus 3000 y 9000 se encuentran afectados por estas vulnerabilidades si ejecutan una versión vulnerable de Cisco NX-OS y cuentan con el shell Bash habilitado o un usuario configurado para usar el shell Bash.

Productos afectados:

- Cisco NX-OS versión 10.4(1) hasta 10.4(3)
- Cisco NX-OS versión 10.3(1) hasta 10.3(5)
- Cisco NX-OS versión 10.1(1) hasta 10.2(7)
- Cisco NX-OS versión 10.1(1) hasta 10.2(7)
- Cisco NX-OS versión 9.2(1) hasta 9.2(13)

Recomendación:

Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco NX-OS. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar las vulnerabilidades.

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bshacepe-bApeHSx7

CVE-2024-20284, CVE-2024-20285 y CVE-2024-20286: Vulnerabilidades en Cisco NX-OS permiten acceso no autorizado**. - (MEDIA)**

El intérprete de Python de Cisco NX-OS cuenta con vulnerabilidades de validación insuficiente de la entrada brindada por el usuario. Esto puede ser aprovechado por un atacante local autenticado y con privilegios de ejecución de Python para manipular funciones específicas dentro del intérprete, escapar del entorno aislado de Python y ejecutar comandos arbitraros en el sistema operativo subyacente con los privilegios del usuario autenticado.

Los switches MDS 9000 Series Multilayer, Nexus 3000 Series, Nexus 5500 Platform, Nexus 5600 Platform, Nexus 6000 Series, Nexus 7000 Series y Nexus 9000 Series están afectados por estas vulnerabilidades si ejecutan una versión vulnerable de Cisco NX-OS.

Productos afectados:

- Cisco NX-OS versión 10.4(1) hasta 10.4(3)
- Cisco NX-OS versión 10.3(1) hasta 10.3(5)
- Cisco NX-OS versión 10.1(1) hasta 10.2(7)
- Cisco NX-OS versión 8.5(1) hasta 9.4(1a)
- Cisco NX-OS versión 8.0(1) hasta 8.4(9)
- Cisco NX-OS versión 6.0(2)A6(1) hasta 7.3(14)N1(1)

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco NX-OS. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar las vulnerabilidades.

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du

CVE-2024-20289: Vulnerabilidad en Cisco NX-OS permite inyección de comandos**. - (MEDIA)**

Se detectó una vulnerabilidad de validación insuficiente de argumentos en la CLI de Cisco NX-OS, el cual puede ser aprovechado por un atacante local autenticado y con pocos privilegios para ejecutar comandos arbitrarios en el sistema operativo subyacente, luego de incluir una entrada creada como argumento en un equipo vulnerable.

Los switches Nexus 3000 Series, Nexus 9000 Series y Fabric Series, además de los interconectores UCS 6400 Series Fabric y UCS 6500 Series Fabric son afectados por la vulnerabilidad Cisco NX-OS si ejecutan una versión vulnerable.

Productos afectados:

- Cisco NX-OS versión 10.4(1) hasta 10.4(2)
- Cisco NX-OS versión 10.3(1) hasta 10.3(4a)
- Cisco NX-OS versión 10.1(1) hasta 10.2(6)
- Cisco NX-OS versión 9.3(3) hasta 9.3(12)

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco NX-OS. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmdinj-Lq6jsZhH

BAFING

CISCO APPLICATION POLICY INFRASTUCTURE CONTROLLER

CVE-2024-20478: Vulnerabilidad en Cisco Application Policy Infrastructure Controller permite elevación de privilegios**. - (MEDIA)**

El componente de actualización de software de Cisco Application Policy Infrastructure Controller (APIC) y Cisco Cloud Network Controller, presenta una vulnerabilidad surgida por una validación insuficiente de firmas de las imágenes de software. Un atacante remoto autenticado con privilegios de nivel administrador puede aprovechar la vulnerabilidad al instalar una imagen de software modificada y ejecutar código arbitrario para elevar sus privilegios a nivel "root".

Productos afectados:

- Cisco Application Policy Infrastructure Controller (APIC) versión 6.0
- Cisco Application Policy Infrastructure Controller (APIC) versión 5.3 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco Application Policy Infrastructure Controller. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-priv-esc-uYQJjnuU

CVE-2024-20279: Vulnerabilidad en Cisco Application Policy Infrastructure Controller permite modificar comportamiento de políticas**. - (MEDIA)**

Una vulnerabilidad de control de acceso inadecuado cuando se utilizan dominios de seguridad en Cisco Application Policy Infrastructure Controller puede ser aprovechada por un atacante remoto, autenticado con una cuenta de usuario asociada a un dominio de seguridad restringido, para leer, modificar o eliminar políticas secundarias creadas bajo políticas predeterminadas del sistema. Esto puede provocar la interrupción del tráfico de la red.

La vulnerabilidad afecta a Cisco APIC cuando tienen configurado dominios de seguridad restringidos con usuarios asociados que tenían permisos de administrador de puertos.

Productos afectados:

- Cisco Application Policy Infrastructure Controller (APIC) versión 6.0
- Cisco Application Policy Infrastructure Controller (APIC) versión 5.3 y anteriores

Recomendación:
Se recomienda validar si la organización cuenta con las versiones vulnerables de Cisco Application Policy Infrastructure Controller. De ser el caso, aplicar las actualizaciones o parches correspondientes para solucionar esta vulnerabilidad.

BAFING

URL asociado:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cousmo-uBpBYGbq

+51 1 225 9900
info@bafing.com
www.bafing.com
Bafing
Av. Del Parque Sur 560, San Borja, Lima,Perú

Ciberseguridad
Smart Buildings
e-Health