Basque CyberSecurity Centre

Vulnerabilidades en productos Cisco

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Cisco, compañía relacionada con el sector de redes y tecnología, ha publicado un total de dieciocho avisos de seguridad, donde destacan nueve que contienen nueve vulnerabilidades calificadas con una severidad alta por parte del fabricante. Dichos errores afectan a Cisco IOS, Cisco IOS XE, Cisco Access Point y Cisco DNA.

Con respecto a los fallos que han sido catalogados con una severidad alta, han sido registrados bajo los siguientes identificadores:

- CVE-2023-20027: vulnerabilidad que puede causar una condición de denegación de servicio (DoS) en Cisco IOS XE.
- CVE-2023-20065: vulnerabilidad que puede resultar en que un atacante local eleve sus privilegios a *root* en Cisco IOS XE.
- CVE-2023-20035: vulnerabilidad que puede provocar una ejecución de código arbitrario en Cisco IOS XE SD-WAN.
- CVE-2023-20072: vulnerabilidad que puede causar una condición de denegación de servicio (DoS) en Cisco IOS XE.
- CVE-2023-20080: vulnerabilidad que puede provocar una condición de denegación de servicio (DoS) en Cisco IOS y Cisco IOS XE.
- CVE-2023-20067: vulnerabilidad que puede resultar en una condición de denegación de servicio (DoS) en Cisco IOS XE.
- CVE-2023-20055: vulnerabilidad que permite a un atacante remoto autenticado elevar privilegios en el contexto de la interfaz de gestión basada en web en Cisco DNA.
- CVE-2023-20082: vulnerabilidad que puede permitir a un atacante local ejecutar código arbitrario en tiempo de arranque y romper la cadena de confianza en Cisco IOS XE.
- CVE-2023-20112: vulnerabilidad cuya explotación puede resultar en una condición de denegación de servicio (DoS) en Cisco Access Point.

El fabricante ya ha publicado las actualizaciones de seguridad correspondientes, corrigiendo de esta manera los fallos destacados, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Análisis técnico

En primera instancia, se detalla la vulnerabilidad identificada bajo el CVE-2023-20027. Dicho fallo existe debido a reensamblaje incorrecto de paquetes en caso de que la función *VFR* esté habilitada. Un atacante remoto puede llegar a enviar los paquetes fragmentados, obligando a recargar el dispositivo, resultando en una condición de denegación de servicio (DoS) en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.6

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

La segunda vulnerabilidad, cuyo identificador es CVE-2023-20065 es un error debido a una implementación de restricciones insuficientes de acceso en el sistema de destino. Un atacante local puede llegar a escalar privilegios, adoptando un rol de *root* en el dispositivo vulnerable.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

Seguidamente, la vulnerabilidad identificada bajo el CVE-2023-20035 es causada debido a una validación insuficiente de entrada en el CLI del sistema, que puede permitir a un atacante con privilegios ejecutar código arbitrario, comprometiendo de esta manera el dispositivo vulnerable.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

El error registrado bajo el CVE-2023-20072 está provocado por la gestión inadecuada de paquetes fragmentados pertenecientes a *tunnel protocol*. Un atacante remoto puede llegar a enviar los paquetes fragmentados, obligando a recargar el dispositivo, resultando en una condición de denegación de servicio (DoS) en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.6

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

El fallo registrado bajo el CVE-2023-20080 existe debido a una validación insuficiente de entrada del límite de los datos. Un atacante remoto puede enviar mensajes *DHCPv6* manipulados, llegando a provocar una condición de denegación de servicio (DoS) en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.6

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

La sexta vulnerabilidad reportada, registrada bajo el CVE-2023-20067 está causado debido a validación insuficiente de entrada del tráfico recibido por parte del sistema de destino. Un atacante remoto puede enviar tráfico especialmente diseñado, pudiendo resultar en una condición de denegación de servicio (DoS) en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.4

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Adyacente**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

Del mismo modo, la vulnerabilidad identificada bajo el CVE-2023-20055 existe debido a la exposición de información confidencial en la API de gestión del sistema. Un atacante remoto puede llegar a evitar las restricciones de seguridad y llevar a cabo una escalada de privilegios tras acceder a la API.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.0

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

El fallo registrado bajo el CVE-2023-20082 se produce debido a errores que se producen al recuperar la clave pública de liberación que se utiliza para la verificación de la firma de la imagen. Un atacante con acceso físico puede modificar variables específicas en la memoria flash de la interfaz periférica serie (SPI) y ejecutar código arbitrario en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 6.1

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

- **Vector de ataque**: Físico
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Ninguna**

Por último, el error identificado como CVE-2023-20112 está causado debido a una validación insuficiente de ciertos parámetros en el sistema de destino. Un atacante remoto puede causar una condición de denegación de servicio (DoS).

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.4

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

- **Vector de ataque**: **Adyacente**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

Finalmente, los productos afectados por las anteriores vulnerabilidades son los siguientes:

- Cisco IOS XE versiones 17.9.1, 17.9.1a y 17.9.1.w.
- Cisco IOS XE ROM Monitor versiones anteriores a 17.6.5r.
- 1000 Series Integrated Services Routers.
- 4000 Series Integrated Services Routers.
- ASR 1000 Series Aggregation Services Routers.
- Catalyst 8000 Edge Platforms Family.
- Catalyst 8000V Edge Software Routers.
- Catalyst 8200 Series Edge Platforms.
- Catalyst 8300 Series Edge Platforms.
- Catalyst 8500L Series Edge Platforms.
- Catalyst 9300 Series Switches.

- Catalyst 9800 Embedded Wireless Controllers para Catalyst 9300, 9400, y 9500 Series Switches.
- Catalyst 9800 Series Wireless Controllers.
- Catalyst 9800-CL Wireless Controllers para Cloud.
- Embedded Wireless Controllers en Catalyst Access Points
- Cloud Services Router 1000V Series.
- Cisco DNA Center con configuración predeterminada.
- Business 150 APs y 151 Mesh Extenders.
- Catalyst 9100 APs.

3. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Aquellos clientes que cuenten con un contrato directo con Cisco deberán recibir las actualizaciones de forma automática según la licencia que dispongan. Para aquellos casos en los que los clientes con productos de la compañía hayan sido adquiridos mediante terceros, deberán ponerse en contacto con el TAC de Cisco a través del siguiente enlace para obtener las correcciones pertinentes:

- Cisco Worldwide Support Contacts.

Con respecto al error CVE-2023-20065, Cisco recomienda a aquellos usuarios que no hagan uso del entorno de hospedaje, que desactiven IOX mediante el comando de configuración *no iox*.

Cabe destacar que, en relación a la vulnerabilidad identificada bajo el CVE-2023-20067, el fabricante recomienda deshabilitar la función de creación de perfiles de cliente HTTP, en caso de que no sea posible aplicar las actualizaciones de seguridad correspondientes. Para ello, los usuarios deberán desmarcar la opción de verificación *Caché HTTP TLV* en todos los perfiles.

4. Referencias Adicionales

- Cisco IOS XE Software Virtual Fragmentation Reassembly Denial of Service Vulnerability.
- Cisco IOS XE Software IOx Application Hosting Environment Privilege Escalation Vulnerability.
- Cisco IOS XE SD-WAN Software Command Injection Vulnerability.
- Cisco IOS XE Software Fragmented Tunnel Protocol Packet Denial of Service Vulnerability.
- Cisco IOS and IOS XE Software IPv6 DHCP (DHCPv6) Relay and Server Denial of Service Vulnerability.
- Cisco IOS XE Software for Wireless LAN Controllers HTTP Client Profiling Denial of Service Vulnerability.
- Cisco DNA Center Privilege Escalation Vulnerability.
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass Vulnerability.
- Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass Vulnerability.
- Cisco Access Point Software Association Request Denial of Service Vulnerability.
- Cisco IOS.
- Cisco IOS XE.
- Cisco Access Point.
- Cisco DNA.
- VRF (Virtual Routing and Forwarding).
- CWE-400: Uncontrolled Resource Consumption.
- CWE-284: Improper Access Control.
- CWE-20: Improper Input Validation.
- CWE-94: Improper Control of Generation of Code ('Code Injection').
- First Organization.
- Cisco Worldwide Support Contact.


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA