Basque CyberSecurity Centre

Vulnerabilidades en productos de 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 siete avisos de seguridad, donde se destaca una vulnerabilidad calificada con una severidad crítica y cuatro errores que cuentan con una puntuación alta. Dichos errores afectan a Cisco Expressway Series, Cisco TelePresence, Cisco Unified Communications Manager IM and Presence Service, Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS, Cisco AnyConnect Secure Mobility Client Software para Windows y Cisco Secure Client Software para Windows.

Con respecto al fallo que ha sido catalogado con una severidad crítica, ha sido registrado bajo el siguiente identificador:

- CVE-2023-20105: vulnerabilidad que puede permitir a un atacante remoto escalar privilegios en Cisco Expressway Series y Cisco TelePresence VCS.

En relación a las vulnerabilidades que han sido calificadas con una severidad alta, han sido identificadas con los siguientes identificadores:

- CVE-2023-20192: vulnerabilidad que puede permitir a un atacante remoto escalar privilegios en Cisco Expressway Series y Cisco TelePresence VCS.
- CVE-2023-20108: vulnerabilidad que puede causar una condición de denegación de servicio (DoS) en Cisco Unified Communications Manager IM and Presence Service.
- CVE-2023-20006: vulnerabilidad que puede causar una condición de denegación de servicio (DoS) en Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS.
- CVE-2023-20178: vulnerabilidad que puede permitir a un atacante remoto escalar privilegios en Cisco AnyConnect Secure Mobility Client Software para Windows y Cisco Secure Client Software para Windows.

El fabricante ya ha publicado las actualizaciones 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 en cuanto se publiquen los parches correspondientes.

2. Análisis técnico

En primera instancia, se detalla la vulnerabilidad identificada bajo el CVE-2023-20105. Dicha vulnerabilidad, calificada con una severidad crítica, existe debido a una gestión inadecuada de las peticiones de cambio de contraseña en la funcionalidad de cambio de contraseña. Un usuario remoto puede enviar una solicitud especialmente diseñada y modificar las contraseñas de cualquier usuario en el sistema y suplantar al usuario objetivo.

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: 9.6

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

- **Vector de ataque**: **Red**.
- **Complejidad del ataque**: **Bajo**.
- **Privilegios requeridos**: **Bajo**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: **Con cambios**.
- **Confidencialidad**: Ninguno.
- **Integridad**: **Alta**.
- **Disponibilidad**: **Alta**.

La segunda vulnerabilidad, cuyo identificador es CVE-2023-20192, es un error que existe debido a una asignación incorrecta de los permisos de rol de usuario. Un usuario local puede ejecutar código arbitrario, con permisos de administrador, en el sistema de destino.

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: 8.4

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

- **Vector de ataque**: Local.
- **Complejidad del ataque**: **Bajo**.
- **Privilegios requeridos**: **Bajo**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: **Con cambios**.
- **Confidencialidad**: Ninguno.

- **Integridad**: **Alta**.
- **Disponibilidad**: **Alta**.

El error registrado bajo el CVE-2023-20108 está provocado debido a la insuficiente validación de la entrada proporcionada por el usuario en el Servicio de Autenticación XCP. Un atacante remoto puede enviar un mensaje de inicio de sesión especialmente diseñado y realizar un ataque de denegación de servicio (DoS).

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen de:

CVSS Base: 7.5

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

- **Vector de ataque**: **Red**.
- **Complejidad del ataque**: **Bajo**.
- **Privilegios requeridos**: **Ninguno**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: Sin cambios.
- **Confidencialidad**: Ninguno.
- **Integridad**: Ninguno.
- **Disponibilidad**: **Alta**.

La cuarta vulnerabilidad, identificada bajo el CVE-2023-20006, existe debido a un error de implementación dentro de las funciones criptográficas para el procesamiento de tráfico SSL/TLS cuando se descargan al hardware. Un atacante remoto puede enviar un flujo de tráfico SSL/TLS especialmente diseñado a un dispositivo afectado y realizar un ataque de denegación de servicio (DoS).

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen 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**: **Bajo**.
- **Privilegios requeridos**: **Ninguno**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: **Con cambios**.

- **Confidencialidad**: Ninguno.
- **Integridad**: Ninguno.
- **Disponibilidad**: **Alta**.

Por último, el error identificado bajo el CVE-2023-20178, está causado debido a una asignación incorrecta de los permisos de rol de usuario durante el proceso de actualización del sistema. Un usuario local puede ejecutar código arbitrario, con permisos de administrador, en el sistema de destino.

Las métricas de evaluación de la vulnerabilidad anteriormente descrita se componen 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**: **Bajo**.
- **Privilegios requeridos**: **Bajo**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: Sin cambios.
- **Confidencialidad**: **Alta**.
- **Integridad**: **Alta**.
- **Disponibilidad**: **Alta**.

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

- Cisco Expressway Series y Cisco TelePresence VCS versión 14.0 y anteriores.
- Cisco Unified Communications Manager IM and Presence Service versiones 12.5(1) y 14SU.
- Cisco Adaptative Security Appliance versiones 9.16.4, 9.18.2 y 9.18.2.5.
- Cisco Firepower Threat Defense versiones 7.2.1, 7.2.2 y 7.2.3.
- Cisco AnyConnect Secure Mobility Client Software para Windows versión 4.10 y anteriores.
- Cisco Secure Client Software para Windows versión 5.0.

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.

Cabe destacar que el fabricante insta a los usuarios que implementen las siguientes versiones en los productos afectados:

- Cisco Expressway Series y Cisco TelePresence VCS versión 14.2.1 o 14.3.0.
- Cisco Unified Communications Manager IM and Presence Service versiones 12.5(1)SU7 o 14SU3.
- Cisco AnyConnect Secure Mobility Client Software para Windows versión 4.10MR7.
- Cisco Secure Client Software para Windows versión 5.0MR2.

4. Referencias Adicionales

- Cisco Security Advisories.
- Cisco Expressway Series, Cisco TelePresence.
- Cisco Unified Communications Manager IM and Presence Service.
- Cisco Adaptative Security Appliance Software and Firepower Threat Defense Software for Firepower 2100 Series Appliances SSL/TLS.
- Cisco AnyConnect Secure Mobility Client Software para Windows.
- Cisco Secure Client Software para Windows.
- CWE-400: Uncontrolled Resource Consumption.
- CWE-620: Unverified Password Change.
- CWE-20: Improper Input Validation.
- Cisco Worldwide Support Contacts.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA