Basque CyberSecurity Centre

Vulnerabilidad en adaptadores telefónicos de Cisco (SPA112 2)

BCSC-AVISOS

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 manera 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. Aviso de seguridad

Cisco ha publicado un aviso de seguridad donde se trata una vulnerabilidad de severidad crítica, cuyo identificador es CVE-2023-20126, que afecta al producto Cisco SPA112 2-Port Phone Adapter, un adaptador de teléfono analógico que permite conectar teléfonos y máquinas de fax a un proveedor de servicios VoIP a través de una red IP. La vulnerabilidad podría permitir que un atacante remoto no autenticado ejecute código arbitrario, de forma que, una explotación exitosa de la misma supondría un alto impacto en la confidencialidad, la integridad y la disponibilidad de los sistemas afectados.

El fabricante no ha publicado, ni publicará, una actualización o workaround para tratar el fallo descrito debido a que el producto se encuentra en el final de su ciclo de vida. Desde Cisco se recomienda a sus clientes a migrar a un adaptador de teléfono analógico de la serie Cisco ATA 190.

2. Recursos afectados

- Todas las versiones de firmware de Cisco SPA112 2-Port Phone Adapters.

3. Análisis técnico

El detalle de la vulnerabilidad tratada en este aviso es el siguiente:

CVE-2023-20126: vulnerabilidad en la interfaz de administración basada en web de los adaptadores de teléfono Cisco SPA112 que podría permitir que un atacante remoto no autenticado ejecute código arbitrario en un dispositivo afectado. El error se debe a la falta de un proceso de autenticación dentro de la función de actualización del firmware. Un atacante podría aprovechar esta vulnerabilidad actualizando un dispositivo afectado a una versión modificada del firmware. Una explotación exitosa podría permitir que el atacante ejecute código arbitrario en el dispositivo afectado con todos los privilegios.

La métrica de evaluación de las vulnerabilidades se compone de:

CVSS Base: 9.8

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

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

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para tratar la vulnerabilidad descrita, y dado que el producto está en el final de su ciclo de vida, desde Cisco se recomienda a sus clientes a migrar a un adaptador de teléfono analógico de la serie Cisco ATA 190.

5. Referencias Adicionales.

- Aviso de seguridad.
- CVE-2023-20126.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA