Basque CyberSecurity Centre

Vulnerabilidad en Switches Aruba CX

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

Aruba ha lanzado actualizaciones de seguridad para ciertos switches cableados que ejecutan el sistema operativo AOS-CX, abordando una vulnerabilidad de severidad alta, cuyo identificador es CVE-2023-1168, en el motor de análisis de red (NAE). El fallo puede llevar a una condición de ejecución remota de código arbitrario creando un alto impacto en la confidencialidad, integridad y disponibilidad de los sistemas afectados.

Cabe destacar que desde Aruba se afirma no tener conocimiento de divulgación pública o código de explotación que apunte a esta vulnerabilidad a fecha de publicación de este aviso.

2. Recursos afectados

Modelos Aruba Switch:

- Aruba CX 10000 Switch Series.
- Aruba CX 9300 Switch Series.
- Aruba CX 8400 Switch Series.
- Aruba CX 8360 Switch Series.
- Aruba CX 8325 Switch Series.
- Aruba CX 8320 Switch Series.
- Aruba CX 6400 Switch Series.
- Aruba CX 6300 Switch Series.
- Aruba CX 6200F Switch Series.

Versiones de software:

- AOS-CX 10.10.xxxx: 10.10.1020 y versiones inferiores.
- AOS-CX 10.09.xxxx: 10.09.1020 y versiones inferiores.
- AOS-CX 10.08.xxxx: 10.08.1070 y versiones inferiores.
- AOS-CX 10.06.xxxx: 10.06.0230 y versiones inferiores.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada son los siguientes:

CVE-2023-1168: vulnerabilidad de ejecución de código remoto autenticado que afecta al motor de análisis de red AOS-CX. La explotación exitosa de esta vulnerabilidad da como resultado la capacidad de ejecutar código arbitrario como un usuario privilegiado en el sistema operativo subyacente, lo que podría conducir a un compromiso completo del switch que ejecuta AOS-CX.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.2

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos
- **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 a vulnerabilidad descrita en el aviso, Aruba recomienda actualizar el software a una de las siguientes versiones:

- AOS-CX 10.11.xxxx: 10.11.0001 y superior.
- AOS-CX 10.10.xxxx: 10.10.1030 y superior.
- AOS-CX 10.06.xxxx: 10.06.0240 y superior.

Se remarca desde Aruba que no se evalúan ni actualizan las versiones de firmware de AOS-CX que hayan alcanzado el fin de soporte, estableciendo como versiones admitidas, a la fecha de publicación de este aviso, las siguientes:

- AOS-CX 10.11.xxxx.
- AOS-CX 10.10.xxxx.
- AOS-CX 10.06.xxxx.

Por último, como medida de mitigación alternativa para minimizar la probabilidad de que un atacante aproveche esta vulnerabilidad, desde Aruba se propone que las interfaces de gestión basadas en CLI y en la web se restrinjan a un segmento/VLAN dedicado de capa 2 y/o sean controladas por políticas de firewall en la capa 3 y superiores.

5. Referencias Adicionales

- Actualizaciones de seguridad.
- CVE-2023-1168.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA