Basque CyberSecurity Centre

Vulnerabilidades en ArubaOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Resumen ejecutivo 4
2. Análisis técnico 5
3. Mitigación / Solución 9
4. Referencias Adicionales 10

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

Aruba, compañía relacionada con diversas soluciones de seguridad, ha publicado un aviso que contiene un total de 33 vulnerabilidades. Entre ellas, se destacan 6 vulnerabilidades que han sido calificadas como críticas por parte del fabricante, además de contar con un total de 19 fallos que se les ha asignado una severidad alta.

Las vulnerabilidades, cuya severidad ha sido catalogada como crítica, han sido registradas bajo los siguientes identificadores:

- CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 y CVE-2023-22750: vulnerabilidades que pueden resultar en la inyección de comandos arbitrarios en *PAPI Protocol*.
- CVE-2023-22751 y CVE-2023-22752: vulnerabilidades que pueden causar un desbordamiento de búfer en *PAPI Protocol*.

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

- CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756 y CVE-2023-22757: vulnerabilidades que pueden causar un desbordamiento de búfer en ArubaOS.
- CVE-2021-3712: vulnerabilidad que puede resultar en un desbordamiento de búfer al procesar *cadenas ASN.1* en ArubaOS.
- CVE-2023-22758, CVE-2023-22759, CVE-2023-22760 y CVE-2023-22761: vulnerabilidades que pueden causar una ejecución de comandos arbitrarios en la interfaz de gestión basada en web de ArubaOS.
- CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769 y CVE-2023-22770: vulnerabilidades que pueden resultar en la ejecución de comandos arbitrarios en la interfaz en línea de comandos de ArubaOS.

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

Con respecto a las vulnerabilidades críticas reportadas por parte de Aruba, se han identificado los errores registrados bajo los CVE-2023-22747, CVE-2023-22748, CVE-2023-22749 y CVE-2023-22750. Dichos fallos, que han reportados por parte del investigador Erik de Jong, existen debido a una validación de entrada incorrecta en *PAPI Protocol*. Un atacante remoto no autenticado puede enviar paquetes especialmente diseñados al puerto 8211/UDP y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

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

Del mismo modo, las vulnerabilidades críticas y registradas bajo los CVE-2023-22751 y CVE-2023-22752, han sido reportadas por parte del investigador Erik de Jong. Dichos errores, están causados por un *boundary error* en *PAPI Protocol*. Un atacante remoto no autenticado puede enviar paquetes especialmente diseñados al puerto 8211/UDP, desencadenar un desbordamiento de búfer y ejecutar código arbitrario en el sistema de destino.

Las métricas de evaluación de las vulnerabilidades CVE-2023-22751 y CVE-2023-22752 se componen 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**: **Bajo**.
- **Privilegios requeridos**: **Ninguno**.
- **Interacción con el usuario**: **Ninguno**.

- **Alcance**: Sin cambios.
- **Confidencialidad**: **Alta**.
- **Integridad**: **Alta**.
- **Disponibilidad**: **Alta**.

En relación a las vulnerabilidades cuya severidad ha sido catalogada como alta, y son identificadas bajo los CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756 y CVE-2023-22757, han sido reportadas por parte del investigador Haoliang Hu. Estos fallos existen debido a un *boundary error* en *PAPI Protocol*. Un atacante remoto puede enviar paquetes especialmente diseñados al puerto 8211/UDP, provocar la corrupción de memoria y ejecutar código arbitrario en el sistema de destino.

Las métricas de evaluación de las vulnerabilidades anteriormente descritas se componen de:

CVSS Base: 8.1

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

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

El error registrado bajo el CVE-2021-3712, catalogado con una severidad alta y que ha sido reportado por Ingo Schwarze, está causado por una condición de límite al procesar *cadenas ASN.1* relacionada con la terminación *NULL*. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación para desencadenar *out-of-bounds read error* y leer contenidos de la memoria del sistema o realizar un ataque de denegación de servicio (DoS).

Las métricas de evaluación de la vulnerabilidad CVE-2021-3712 se compone de:

CVSS Base: 7.4

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

- **Vector de ataque**: **Red**.
- **Complejidad del ataque**: Alto.

- **Privilegios requeridos**: **Ninguno**.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: Sin cambios.
- **Confidencialidad**: **Alta**.
- **Integridad**: Ninguno.
- **Disponibilidad**: **Alta**.

Del mismo modo, los errores registrados bajo los CVE-2023-22758, CVE-2023-22759, CVE-2023-22760 y CVE-2023-22761, han sido puntuados con una criticidad alta. Estas vulnerabilidades, reportadas inicialmente por parte de Daniel Jensen, Erik de Jong y Nikita Abramov, existen debido a una validación de entrada inadecuada en la interfaz de gestión basada en web. Un usuario remoto autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

Las métricas de evaluación de las vulnerabilidades anteriormente descritas se componen 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**: **Bajo**.
- **Privilegios requeridos**: Alto.
- **Interacción con el usuario**: **Ninguno**.
- **Alcance**: Sin cambios.
- **Confidencialidad**: **Alta**.
- **Integridad**: **Alta**.
- **Disponibilidad**: **Alta**.

Por último, las vulnerabilidades identificadas bajo los CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769 y CVE-2023-22770, también han sido calificadas con una criticidad alta por parte del fabricante. Dichos fallos, reportados por Daniel Jensen y Erik de Jong, están causados por una validación de entrada inadecuada en la interfaz en línea de comandos de ArubaOS. Un usuario local puede pasar argumentos especialmente diseñados a través de la interfaz afectada y ejecutar comandos arbitrarios del sistema operativo en el sistema de destino.

Las métricas de evaluación de las vulnerabilidades anteriormente descritas se componen 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**: **Bajo**.
- **Privilegios requeridos**: Alto.
- **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:

- ArubaOS versión 8.6.0.19 y anteriores, 8.10.0.4 y anteriores y 10.3.1.0 y anteriores.
- SD-WAN versión 8.7.0.0-2.3.0.8 y anteriores.

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.

Para ello, se deberá actualizar ArubaOS a las siguientes versiones destacadas:

- ArubaOS 8.10.XX: actualizar a la versión 8.10.0.5 o superior.
- ArubaOS 8.11.XX: actualizar a la versión 8.11.0.0 o superior.
- ArubaOS 10.3.XX: actualizar a la versión 10.3.1.1 o superior.

En relación a SD-WAN, se deberá instalar la versión 8.7.0.0-2.3.0.9 o superior, con la finalidad de aplicar la solución oficial propuesta por el fabricante.

En adición a lo anterior, Aruba ha dado a conocer medidas alternativas de seguridad, que deberán ser aplicadas por aquellos administradores que no puedan llegar a implementar las soluciones anteriormente descritas, o que cuenta con una versión que se encuentre fuera de soporte.

En relación a las vulnerabilidades CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750, CVE-2023-22751, CVE-2023-22752, CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756 y CVE-2023-22757, los usuarios deberán habilitar la función *PAPI Security* con una clave que no sea la predeterminada.

Con respecto a los fallos registrados bajos los CVE-2023-22758, CVE-2023-22759, CVE-2023-22760 y CVE-2023-22761, se deberá bloquear, para aquellos usuarios que no sean de confianza, el acceso a la interfaz de administración basada en web de ArubaOS.

Por último, para aplicar la mitigación alternativa de seguridad que afecta a las vulnerabilidades identificadas como CVE-2021-3712, CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769 y CVE-2023-22770, se deberá restringir la comunicación entre el componente *Controller* y los puntos de acceso.

4. Referencias Adicionales

- ARUBA-PSA-2023-002.
- PAPI Protocol.
- ArubaOS.
- SD-WAN.
- Puerto 8211/UDP.
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').
- Boundary error.
- CWE-121: Stack-based Buffer Overflow.
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.
- CWE-125: Out-of-bounds Read.
- ¿Qué son los ataques DoS y DDoS?
- CWE-20: Improper Input Validation.
- ArubaOS 8.X Command-Line Interface.
- ArubaOS 8.10.0.5 Release Notes.
- ArubaOS 8.11.0.0 Release Notes.
- AOS 10.3.1.1 Release Notes.
- Updating Software Images on Aruba Gateways.
- PAPI Security.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA