Vulnerabilidades en ArubaOS

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca 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 la Agencia de Ciberseguridad Vasca. 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.

1. Resumen ejecutivo

Aruba network ha publicado un aviso de seguridad corrigiendo **múltiples vulnerabilidades** que afectan a los productos **ArubaOS**, sistema operativo desarrollado por Aruba Networks y al software **SD-WAN**, la red de área local definida por software SD-WAN.

Entre las más significativas se encuentran **4 vulnerabilidades de severidad alta,** CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613, las cuales podrían permitir a usuarios remotos autenticados, ejecutar comandos arbitrarios como root en el host subyacente y comprometer el sistema al completo, representando, todas ellas, una amenaza de alta gravedad para la confidencialidad, integridad y disponibilidad en los sistemas que se puedan ver afectados por su explotación.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación 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. Recursos afectados

Las siguientes **versiones de ArubaOS** están afectadas por las vulnerabilidades expuestas:

- ArubaOS 10.5.x.x: 10.5.0.1 e inferiores
- ArubaOS 10.4.x.x: 10.4.0.3 e inferiores
- ArubaOS 8.11.x.x: 8.11.2.0 e inferiores
- ArubaOS 8.10.x.x: 8.10.0.9 e inferiores

Así mismo, cabe destacar que hay versiones de ArubaOS y SD-WAN que han alcanzado el final de su mantenimiento y están afectadas por estas vulnerabilidades, pero no están corregidas por esta actualización, son las siguientes:

- ArubaOS 10.3.x.x: todas las versiones
- ArubaOS 8.9.x.x: todas las versiones
- ArubaOS 8.8.x.x: todas las versiones
- ArubaOS 8.7.x.x: todas las versiones
- ArubaOS 8.6.x.x: todas las versiones
- ArubaOS 6.5.4.x: todas las versiones
- SD-WAN 8.7.0.0-2.3.0.x: todas las versiones
- SD-WAN 8.6.0.4-2.2.x.x: todas las versiones

Cualquier otro producto de HPE Aruba Networking que no figure específicamente en la lista anterior, no se ve afectado por estas vulnerabilidades.

3. Análisis técnico

Los detalles de las vulnerabilidades de más relevancia tratadas en este aviso son los siguientes:

CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613: vulnerabilidades de inyección de comandos autenticados que afectan a la interfaz de línea de comandos de ArubaOS. La explotación de estas vulnerabilidades podría posibilitar la ejecución de comandos arbitrarios como usuario privilegiado en el sistema operativo subyacente.

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 del usuario: Ninguna**
- **Ámbito de aplicación:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. 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.

HPE Aruba recomienda actualizar los Controladores de Movilidad, Conductores de Movilidad y Pasarelas a una de las siguientes versiones de ArubaOS:

- ArubaOS 10.5.x.x: 10.5.1.0 y superior.
- ArubaOS 10.4.x.x: 10.4.1.0 y superior.
- ArubaOS 8.11.x.x: 8.11.2.1 y superior.
- ArubaOS 8.10.x.x: 8.10.0.10 y superior.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2024-1356.
- CVE-2024-25611.
- CVE-2024-25612.
- CVE-2024-25613.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY