USTIC-AV 17/22. Vulnerabilidad crítica en productos Aruba (04/11/2022)

La **Unidad de Seguridad TIC** de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** de la **publicación** de una **vulnerabilidad crítica de inyección de comandos** en productos **Aruba.**

Detalle

Se han identificado 16 vulnerabilidades, una de ellas de severidad crítica, que afectan a productos Aruba (subsidiaria de HP), cuya explotación podría permitir a un atacante inyectar código, ejecutar código arbitrario de forma remota, modificar la secuencia de arranque, eliminar archivos arbitrarios, causar una condición de denegación de servicio, divulgar información sensible, desbordar el búfer o lectura de archivos arbitrarios.

Para la vulnerabilidad **catalogada como crítica**, se le ha asignado el identificador **CVE-2022-37897**, con una puntuación de CVSSv3: 9,8. **Podría conducir a la ejecución de código remoto no autenticado mediante el envío de paquetes especialmente diseñados destinados al puerto UDP (8211) de PAPI** (protocolo de gestión de AP de Aruba Networks). **La explotación exitosa** de esta vulnerabilidad **podría** resultar en la capacidad de **ejecutar código arbitrario como un usuario privilegiado en el sistema** operativo subyacente.

Recursos Afectados

- Aruba Mobility Conductor (conocido anteriormente como *Mobility Master*).
- Aruba Mobility Controllers.
- WLAN Gateways y SD-WAN Gateways gestionados por Aruba Central.
- ArubaOS, versiones:
    - 5.4.22 y anteriores;
    - 6.0.17 y anteriores;
    - 7.1.9 y anteriores;
    - 3.0.0.
- SD-WAN, versiones desde 8.7.0.0 hasta 2.3.0.6 y anteriores.
- Todas las versiones de los productos EOL:
    - ArubaOS 8.4.x.x;
    - ArubaOS 8.5.x.x;
    - ArubaOS 8.8.x.x;
    - ArubaOS 8.9.x.x;
    - SD-WAN 8.5.0.0-2.1.x.x;
    - SD-WAN 8.6.0.4-2.2.x.x.

Recomendaciones Actualizadas (04/11/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas:

Mitigación

1º. Solución a las vulnerabilidades:

- **Actualizar** los productos afectados a las versiones:
    - ArubaOS 6.5.4.23 y superiores;
    - ArubaOS 8.6.0.18 y superiores;
    - ArubaOS 8.7.1.10 y superiores;
    - ArubaOS 8.10.0.0 y superiores;
    - ArubaOS 10.3.0.1 y superiores;
    - SD-WAN 8.7.0.0-2.3.0.7 y superiores.

Referencias

- Aviso Oficial Aruba: Document - HPESBNW04381 rev.1 - Aruba SD-WAN Software and Gateways, Multiple Vulnerabilities | HPE Support
- ARUBA-PSA-2022-016

En caso de haber detectado la explotación de estas vulnerabilidades :

debe reportar el incidente mediante correo electrónico a ayudadigital.sspa@juntadeandalucia.es in dicando en el *Asunto: [Compromiso Aruba0411]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud