BOLETÍN DE ALERTA

Boletín Nro.: 2022-45
Fecha de publicación: 27/10/2022
Tema: Vulnerabilidades críticas en productos Aruba

Algunos productos afectados son:

- ArubaOS 6.5.4.x: versiones 6.5.4.22 y anteriores.
- ArubaOS 8.6.x.x: versiones 8.6.0.17 y anteriores.
- ArubaOS 8.7.x.x: versiones 8.7.1.9 y anteriores.
- ArubaOS 10.3.x.x: versión 10.3.0.0.

Puede acceder a la lista completa de los productos afectados en el siguiente enlace.

Descripción:

Aruba Networks ha publicado un aviso de seguridad sobre múltiples vulnerabilidades que afectan a sus productos, que permitirían a un atacante realizar ejecución remota de código (*RCE*), divulgación de información, denegación de servicios (*DoS*), entre otros.

- CVE-2022-37897, de severidad "crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en el protocolo de gestión de AP de Aruba Networks. Esto permitiría a un atacante no autenticado realizar ejecución remota de código (*RCE*) como un usuario privilegiado en el sistema operativo subyacente.

- CVE-2022-37898, de severidad "alta" y con puntuación asignada de 7.2. Esta vulnerabilidad se debe a una falla de seguridad en la interfaz de línea de comandos de ArubaOS. Esto permitiría a un atacante autenticado realizar ejecución remota de código (*RCE*) como un usuario privilegiado en el sistema operativo subyacente.

- CVE-2022-37903, de severidad "alta" y con puntuación asignada de 7.2. Esta vulnerabilidad se debe a una falla de seguridad en la interfaz web de ArubaOS. Esto permitiría a un atacante autenticado sobrescribir archivos arbitrarios en el sistema y realizar ejecución remota de código (*RCE*).

Puede acceder a la lista completa de las vulnerabilidades en el siguiente enlace.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar ejecución remota de código (*RCE*), divulgación de información, denegación de servicios (*DoS*), entre otros.

Solución:

Recomendamos acceder a las actualizaciones provistas por el proveedor en los siguientes enlaces de acuerdo a la versión afectada:

- ArubaOS 6.5.4.23
- ArubaOS 8.6.0.18
- ArubaOS 8.7.1.10
- ArubaOS 8.10.0.0
- SD-WAN 8.7.0.0-2.3.0.7

Mitigación temporal:

Adicionalmente, de manera a reducir la probabilidad de que un atacante explote estas vulnerabilidades, se recomienda que la comunicación entre el *Controller/Gateways* y los *Access-Points* estén restringidos. Además, habilitar la función de seguridad del protocolo de gestión de AP de Aruba Networks *(Enhanced PAPI Security feature*).

Información adicional:

- https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-016.txt
- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04381en_us
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-productos-aruba-0
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37897
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37898
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37903
- https://asp.arubanetworks.com/downloads