USTIC-AV 04/22. Vulnerabilidades críticas en switches de Aruba (10/05/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones avisa de la publicación el pasado 4 de mayo de 2022 de **dos vulnerabilidades** catalogadas como **críticas** que afectan a **dispositivos Aruba** y que **permitirían la ejecución remota de código.**

Detalle

El equipo de investigación de Armis ha descubierto **vulnerabilidades de desbordamiento de búfer basado en memoria dinámica (heap), en el firmware de ArubaOS-Switch y en la biblioteca criptográfica Mocana**, en el firmware de ArubaOS-Switch, que **podrían permitir a un atacante remoto la ejecución de código arbitrario en el dispositivo afectado.**

La explotación de estas vulnerabilidades requiere la interacción de un switch afectado con una fuente de mensajes de desafío de acceso RADIUS controlada por un atacante. Debido a esto, la explotación de estas vulnerabilidades probablemente ocurriría como parte de una cadena de ataque que se basa en la explotación previa de la infraestructura controlada por el cliente.

Se han asignado los identificadores CVE-2022-23676 y CVE-2022-23677 para estas vulnerabilidades y se han catalogado como **críticas**.

Debido a la criticidad, rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad.

Recursos Afectados

- **Aruba Switch Models:**
  - Aruba 5400R Series,
  - Aruba 3810 Series,
  - Aruba 2920 Series,
  - Aruba 2930F Series,
  - Aruba 2930M Series,
  - Aruba 2530 Series,
  - Aruba 2540 Series.

- **Versiones de Software:**
  - ArubaOS-Switch 15.xx.xxxx, todas las versiones;
  - ArubaOS-Switch 16.01.xxxx, todas las versiones;
  - ArubaOS-Switch 16.02.xxxx, versión K.16.02.0033 y anteriores;
  - ArubaOS-Switch 16.03.xxxx, todas las versiones;
  - ArubaOS-Switch 16.04.xxxx, todas las versiones;
  - ArubaOS-Switch 16.05.xxxx, todas las versiones;
  - ArubaOS-Switch 16.06.xxxx, todas las versiones;
  - ArubaOS-Switch 16.07.xxxx, todas las versiones;
  - ArubaOS-Switch 16.08.xxxx, versión KB/WB/WC/YA/YB/YC.16.08.0024 y anteriores;
  - ArubaOS-Switch 16.09.xxxx, versión KB/WB/WC/YA/YB/YC.16.09.0019 y anteriores;
  - ArubaOS-Switch 16.10.xxxx, versión KB/WB/WC/YA/YB/YC.16.10.0019 y anteriores;
  - ArubaOS-Switch 16.11.xxxx, versión KB/WB/WC/YA/YB/YC.16.11.0003 y anteriores.

Recomendaciones Actualizadas (10/05/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos:

Mitigación

1º. Solución a las vulnerabilidades:

Actualizar:

- ArubaOS-Switch 16.02.xxxx, a la versión K.16.02.0034 y superior;
- ArubaOS-Switch 16.08.xxxx, a la versión KB/WB/WC/YA/YB/YC.16.08.0025 o superior;
- ArubaOS-Switch 16.09.xxxx, a la versión KB/WB/WC/YA/YB/YC.16.09.0020 o superior;
- ArubaOS-Switch 16.10.xxxx, a la versión KB/WB/WC/YA/YB/YC.16.10.0020 o superior;
- ArubaOS-Switch 16.11.xxxx, a la versión KB/WB/WC/YA/YB/YC.16.11.0004 o superior;

El resto de productos se actualizarán próximamente. Se informará en esta misma entrada.

Referencias

- Aruba Product Security Advisory: ARUBA-PSA-2022-008
- HPESBNW04291 rev.1 - Aruba Switches, Remote Arbitrary Code Execution

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indic ando en el *Asunto: [Compromiso Aruba0522]*

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

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud