HPE Aruba Networking (anteriormente conocida como Aruba Networks) ha lanzado actualizaciones de seguridad para abordar vulnerabilidades críticas que afectan a ArubaOS y que podrían conducir a la ejecución remota de código (RCE) en sistemas afectados.

De las 10 fallas de seguridad identificadas, cuatro han sido calificadas como críticas en términos de su gravedad:

- CVE-2024-26304 (puntuación CVSS: 9.8) – Vulnerabilidad de desbordamiento de búfer no autenticado en el servicio de gestión L2/L3, accesible a través del protocolo PAPI.
- CVE-2024-26305 (puntuación CVSS: 9.8) – Vulnerabilidad de desbordamiento de búfer no autenticado en el demonio de utilidad, accesible a través del protocolo PAPI.
- CVE-2024-33511 (puntuación CVSS: 9.8) – Vulnerabilidad de desbordamiento de búfer no autenticado en el servicio de informes automáticos, accesible a través del protocolo PAPI.
- CVE-2024-33512 (puntuación CVSS: 9.8) – Vulnerabilidad de desbordamiento de búfer no autenticado en la base de datos de autenticación de usuarios locales, accesible a través del protocolo PAPI.

Un actor de amenazas podría aprovechar estas vulnerabilidades de desbordamiento de búfer enviando paquetes especialmente diseñados al puerto UDP de la Interfaz de Programación de Aplicaciones de Proceso (PAPI), lo que podría permitir la ejecución de código arbitrario como usuario privilegiado en el sistema operativo subyacente.

Estas vulnerabilidades afectan a Mobility Conductor (anteriormente conocido como Mobility Master), Controladores de Movilidad y Pasarelas WLAN y Pasarelas SD-WAN administradas por Aruba Central. Se han identificado en las siguientes versiones de software:

- ArubaOS 10.5.1.0 y versiones anteriores.
- ArubaOS 10.4.1.0 y versiones anteriores.
- ArubaOS 8.11.2.1 y versiones anteriores.
- ArubaOS 8.10.0.10 y versiones anteriores.
- También impactan en las versiones de software ArubaOS y SD-WAN que han alcanzado

el estado de fin de mantenimiento:

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

Un investigador de seguridad identificado como Chancen ha sido reconocido por descubrir y reportar siete de las 10 vulnerabilidades, incluidas las cuatro vulnerabilidades críticas de desbordamiento de búfer.

Se recomienda a los usuarios que apliquen las últimas correcciones disponibles para mitigar posibles amenazas. Como solución temporal para ArubaOS 8.x, se sugiere que los usuarios habiliten la función de seguridad PAPI mejorada utilizando una clave no predeterminada.