Hewlett Packard Enterprise (HPE) ha lanzado actualizaciones de seguridad para corregir diversas vulnerabilidades en productos de puntos de acceso de Aruba Networking, entre las cuales se encuentran dos fallas críticas que podrían permitir la ejecución de comandos sin autenticación.

Estas vulnerabilidades afectan a los puntos de acceso que operan con Instant AOS-8 y AOS-10:

- AOS-10.4.x.x: 10.4.1.4 y versiones anteriores
- Instant AOS-8.12.x.x: 8.12.0.2 y anteriores
- Instant AOS-8.10.x.x: 8.10.0.13 y anteriores

Entre las seis vulnerabilidades recientemente parcheadas, las más graves son CVE-2024-42509 (puntuación CVSS: 9.8) y CVE-2024-47460 (puntuación CVSS: 9.0). Estas fallas críticas en el servicio CLI permiten la inyección de comandos sin autenticación, lo que podría derivar en la ejecución de código arbitrario.

> *«Una vulnerabilidad de inyección de comandos en el servicio CLI subyacente podría permitir la ejecución remota de código sin autenticación mediante el envío de paquetes especialmente diseñados al puerto UDP (8211) del protocolo PAPI de gestión de puntos de acceso de Aruba,»* explicó HPE en un comunicado sobre ambas fallas.
>
> *«La explotación exitosa de esta vulnerabilidad permite la ejecución de código arbitrario como usuario privilegiado en el sistema operativo del dispositivo.»*

Para mitigar CVE-2024-42509 y CVE-2024-47460 en dispositivos que usan Instant AOS-8, se recomienda habilitar la seguridad de clúster mediante el comando *cluster-security*. Sin embargo, para los dispositivos AOS-10, HPE sugiere bloquear el acceso al puerto UDP 8211 desde redes no confiables.

HPE también ha solucionado otras cuatro vulnerabilidades:

- CVE-2024-47461 (puntuación CVSS: 7.2) – Ejecución remota de comandos arbitrarios autenticada en Instant AOS-8 y AOS-10
- CVE-2024-47462 y CVE-2024-47463 (puntuaciones CVSS: 7.2) – Vulnerabilidad de creación de archivos arbitrarios en Instant AOS-8 y AOS-10 que permite la ejecución remota de comandos con autenticación
- CVE-2024-47464 (puntuación CVSS: 6.8) – Vulnerabilidad de recorrido de directorios autenticada que posibilita el acceso remoto no autorizado a archivos

Como medidas adicionales, se aconseja restringir el acceso a las interfaces de administración basadas en CLI y web mediante su colocación en una VLAN dedicada y su control a través de políticas de firewall en la capa 3 y superiores.

> *«Si bien no se ha informado de ataques conocidos que exploten puntos de acceso de Aruba Network, estos dispositivos son atractivos para los ciberdelincuentes debido al acceso potencial que las vulnerabilidades ofrecen mediante ejecución remota de comandos con privilegios elevados. Además, es posible que los actores de amenazas intenten revertir los parches para explotar sistemas que no hayan sido actualizados en el corto plazo»*, señaló Arctic Wolf.