ALERTA

COLCERT AL-1005-025

Vulnerabilidades Producto

”HPE Aruba Networking ha publicado actualizaciones de seguridad críticas para abordar vulnerabilidades en ArubaOS”

Ejecución remota de código (RCE)

Estas vulnerabilidades podrían permitir la ejecución remota de código (RCE) en dispositivos afectados, las cuales podrían ser explotadas por actores maliciosos para tomar el control de los dispositivos y ejecutar código arbitrario.

Dispositivos Afectados

Mobility Conductor (anteriormente Mobility Master)
Mobility Controllers WLAN Gateways SD-WAN Gateways Versiones específicas de ArubaOS
Incluye versiones 10.5.1.0 y anteriores, 8.11.2.1 y anteriores

Impacto en la seguridad digital

Toma de control de dispositivos: Los atacantes podrían tomar el control completo de los dispositivos ArubaOS afectados, lo que les permitiría acceder a datos confidenciales, interrumpir operaciones, instalar malware o realizar otras acciones maliciosas.
Daños a la reputación: Las organizaciones que utilizan dispositivos ArubaOS afectados podrían sufrir daños a su reputación si se produce una brecha de seguridad.

NIVEL DE RIESGO

MEDIO

Para protegerse contra estas vulnerabilidades

Aplicar las actualizaciones de seguridad: Se recomienda a los usuarios aplicar las últimas actualizaciones de seguridad proporcionadas por HPE Aruba Networking.
Habilitar la función de seguridadmejorada de PAPI: Como solución temporal para ArubaOS 8.x.
Monitorización de la red: Acciones para la detección activa de vulnerabilidades

FUENTES:

https://securityaffairs.com/162663/security/hpe-aruba-networking-critical-flaws.html
https://www.theregister.com/2024/05/02/hpe_aruba_patches/
https://www.bleepingcomputer.com/news/security/hpe-aruba-networking-fixes-four-critical-rce-flaws-in-arubaos/

Es importante que los usuarios apliquen las actualizaciones de seguridad lo antes posible y tomen medidas para mitigar el riesgo de explotación.

COLCERT