HPE تصدر تحديثات لثماني ثغرات بأعلى درجات الخطورة في ArubaOS تتيح تجاوز المصادقة وتنفيذ الأوامر عن بُعد



أصلحت HPE 72 ثغرة في ArubaOS، منها ثماني ثغرات بأعلى درجات الخطورة تؤثر في AOS-8 وAOS-10. لا تشير الشركة إلى استغلال فعلي أو شيفرة استغلال علنية حتى الآن، وتوصي بالتحديث العاجل وتقييد الوصول الإداري.

- أصلحت HPE 72 ثغرة في ArubaOS، بينها ثماني ثغرات مصنفة بأعلى درجات الخطورة.
- تؤثر الثغرات الثماني في إصدارات متعددة من AOS-8 وAOS-10، ويمكن استغلالها عن بُعد دون صلاحيات أو تفاعل من المستخدم.
- تشمل تجاوز المصادقة وحقن الأوامر وحقن SQL وفيض الذاكرة المؤقتة، ويؤدي عدد منها إلى تنفيذ شيفرة عن بُعد (من CVE-2026-79844 إلى CVE-2026-79851).
- تفيد HPE بعدم علمها بشيفرة استغلال علنية أو باستغلال فعلي وقت صدور النشرة.

- توصي HPE بحصر واجهات الإدارة (CLI والويب) في شريحة VLAN مخصصة من الطبقة الثانية أو بسياسات جدران نارية.

أصدرت HPE تحديثات أمنية لمعالجة 72 ثغرة في نظام Aruba Operating System (المعروف أيضاً باسم ArubaOS أو AOS)، وهو النظام الذي تعمل عليه البنية اللاسلكية المؤسسية من Aruba Networking، مثل mobility conductors ونقاط الوصول والمتحكمات والبوابات. وتحمل ثماني من هذه الثغرات أعلى تصنيف للخطورة.

ما الذي تأثر

تؤثر الثغرات الثماني في إصدارات متعددة من AOS-8 وAOS-10. ويمكن لمهاجم عن بُعد دون أي صلاحيات استغلالها بهجمات منخفضة التعقيد لا تتطلب تفاعل المستخدم. وتشمل تجاوز المصادقة (ومنه ثغرة في بروتوكول PAPI ضمن AOS-10)، وحقن الأوامر وحقن SQL دون مصادقة في AOS-8، وفيض الذاكرة المؤقتة دون مصادقة في AOS-10. ويؤدي عدد منها إلى تنفيذ شيفرة عن بُعد. وهي مسجلة من CVE-2026-79844 إلى CVE-2026-79851.

حالة الاستغلال وإرشادات الشركة

تذكر HPE أنها لا تعلم بنقاش علني أو شيفرة استغلال تستهدف هذه الثغرات، ولا تملك دليلًا على استغلالها فعلياً حتى تاريخ النشرة. ومع ذلك تحث العملاء بقوة على التحديث نظراً لتعقيد الثغرات واتساعها وأثرها.

وكإجراء تخفيفي، توصي الشركة بحصر واجهات الإدارة (سطر الأوامر والويب) في شريحة VLAN مخصصة من الطبقة الثانية، و/أو التحكم بها عبر سياسات جدران نارية على الطبقة الثالثة وما فوقها، مع ضوابط محاسبة لتتبع أنشطة المستخدمين واستخدام الموارد وتسجيلها.

لماذا يهم ذلك

تقع المتحكمات والبوابات اللاسلكية قريباً من قلب الشبكة. وينبغي للجهات التي تشغّل AOS-8 أو AOS-10 التعامل مع هذا التحديث كأولوية، رغم عدم الإبلاغ عن استغلال، لأن غياب شيفرة الاستغلال العلنية غالباً ما يكون مؤقتاً.

ما يجب فعله الآن

1. حصر جميع أجهزة Aruba التي تعمل بـ AOS-8 أو AOS-10 وتحديد الإصدارات المتأثرة بالرجوع إلى نشرة HPE.
2. جدولة تحديثات HPE وتطبيقها كتغيير عاجل، بدءاً بالمتحكمات المكشوفة للإنترنت أو ضعيفة العزل.
3. حصر واجهات الإدارة (CLI والويب) في شريحة VLAN مخصصة من الطبقة الثانية و/أو بقواعد جدار ناري على الطبقة الثالثة وما فوقها.
4. تفعيل المحاسبة وتسجيل الأنشطة الإدارية ومراجعة السجلات بحثاً عن وصول غير متوقع لواجهات الإدارة.
5. توثيق التعرض والمعالجة ضمن إدارة الثغرات ومتابعة أي تقارير لاحقة عن الاستغلال.