Broadcom تصدر تحديثات لثغرات حرجة في ESX وvCenter ضمن 23 إصلاحًا لمنتجات VMware



أصدرت Broadcom تحديثات لمعالجة 23 ثغرة في منتجات VMware، منها ثغرات حرجة في ESX وvCenter. لا يذكر المصدر استغلالاً فعليًا معروفًا، علمًا أن الشركة لا تشير إليه دائمًا في نشراتها.

- تعالج تحديثات vCenter سبع ثغرات، منها CVE-2026-123903 وهي تجاوز للمصادقة في VMware Directory Service بدرجة CVSS تبلغ 9.8.
- تعالج تحديثات ESX سبع مشكلات، ثلاث منها حرجة وتتيح تنفيذ شيفرة على المضيف: CVE-2026-123910 وCVE-2026-123911 وCVE-2026-123912.
- شملت التحديثات أيضًا ثماني ثغرات في Avi Load Balancer وثغرة في VMware Tools.
- يتضمن إصدار vCenter 8.0 U3m الصادر الأسبوع الماضي بعض الإصلاحات؛ أما vCenter 9.1.x وESX وVMware Tools وFusion وWorkstation وAvi Load Balancer فتحتاج إلى تحديث.
- التحديثات تراكمية، لكن النشرة لا تتناول تحديثات SDDC Manager الواردة في

VMSA-2026-0009.

أصدرت Broadcom تحديثات لمعالجة 23 ثغرة في عدد من منتجات VMware، من بينها ثغرات حرجة في ESX وvCenter.

ما الذي جرى إصلاحه

تعالج تحديثات vCenter سبع ثغرات، أخطرها **CVE-2026-123903** وهي تجاوز للمصادقة في VMware Directory Service بدرجة CVSS تبلغ 9.8. وتشمل الإصلاحات كذلك ثلاث ثغرات حجب خدمة في الخدمة نفسها، وارتقاء محليًا للصلاحيات في أحد سكربتات خدمة vpxd، وكتابة ملفات اعتباطية عند معالجة أرشيفات معينة، وإخفاقًا في فرض السياسات الأمنية في vSphere Distributed Switch.

وتعالج تحديثات ESX سبع مشكلات، ثلاث منها حرجة وقد تؤدي إلى تنفيذ شيفرة على المضيف: CVE-2026-123910 وCVE-2026-123911 (بدرجة 9.8) في خدمة I/O filter، وCVE-2026-123912 (بدرجة 9.3) في وحدة التحكم XHCI USB، وتتطلب صلاحيات إدارية محلية على الجهاز الافتراضي. وتفيد Broadcom بأن الاستغلال على ESX يبقى محصورًا داخل بيئة VMX المعزولة.

كما شملت التحديثات ثماني ثغرات في Avi Load Balancer، بعضها يتيح تنفيذ شيفرة بصلاحيات الجذر، وثغرة حجب خدمة في VMware Tools.

ما الذي يلزم تحديثه

يتضمن vCenter 8.0 U3m، الصادر الأسبوع الماضي، بعض هذه الإصلاحات، ولا حاجة لتحديث إضافي لمن طبّقه. أما vCenter 9.1.x وESX وVMware Tools وFusion وWorkstation وAvi Load Balancer فتتطلب تحديثًا. والتحديثات تراكمية وتشمل إصلاحات VMSA-2026-0009، غير أن هذه النشرة لا تتناول تحديثات SDDC Manager الواردة في تلك النشرة، ويجب معالجتها بصورة مستقلة.

لا تذكر Broadcom استغلالاً فعليًا للثغرات، لكن المصدر يشير إلى أن الشركة كثيرًا ما لا تنبّه إليه في نشراتها العلنية. لذا ينبغي اعتبار غياب التحذير سببًا للمبادرة بالتحديث لا لتأجيله.

ما يجب فعله الآن

1. حصر جميع نسخ vCenter وESX وVMware Tools وFusion وWorkstation وAvi Load Balancer وتوثيق إصداراتها.
2. التحقق من تطبيق vCenter 8.0 U3m، وإعطاء الأولوية لتحديث vCenter 9.1.x ومضيفات ESX.
3. مراجعة نشرة Broadcom وجدولة التحديثات عبر إجراءات إدارة التغيير، مع تقديم الثغرات الحرجة.
4. التأكد من معالجة تحديثات SDDC Manager الواردة في VMSA-2026-0009 لأن هذه النشرة لا تغطيها.
5. تقييد الوصول الإداري إلى واجهات إدارة vCenter وAvi Load Balancer إلى حين اكتمال التحديث.
6. توثيق حالة التحديث وأي استثناءات لأغراض التقارير وفق ضوابط إدارة الثغرات في ضوابط NCA ECC وإطار SAMA CSF.