Broadcom تصدر تحديثات لثغرة حرجة في VMware vCenter Server تتيح تجاوز المصادقة واستُغلت منذ سبتمبر 2026



أصدرت Broadcom تحديثات لثغرة حرجة في VMware vCenter Server تتيح تجاوز المصادقة، وتفيد التقارير بأن جهات مرتبطة بالصين استغلتها كثغرة يوم صفر منذ سبتمبر 2026.

- الثغرة من نوع تجاوز المصادقة وتصنيفها حرج في VMware vCenter Server.
- أصدرت Broadcom تحديثات أمنية لمعالجتها.
- استُغلت كثغرة يوم صفر، وفق المصدر، منذ سبتمبر 2026.
- ينسب المصدر الهجمات إلى مهاجمين مرتبطين بالصين.
- المقتطف المتاح من المصدر لا يتضمن رقم CVE ولا تفاصيل الإصدارات المتأثرة.

أصدرت Broadcom، المالكة الحالية لـ VMware، تحديثات أمنية لثغرة حرجة في vCenter Server تتيح تجاوز المصادقة. ووفق ما نقله موقع BleepingComputer، فإن مهاجمين مرتبطين بالصين يستغلون الثغرة كثغرة يوم صفر منذ سبتمبر 2026، أي أن الهجمات بدأت قبل توفر الإصلاح.

أهمية الخبر

يُعد vCenter Server نقطة الإدارة المركزية للبيئات الافتراضية. وتجاوز المصادقة في نظام كهذا قد يتيح للمهاجم التحرك دون بيانات اعتماد صحيحة، ما يجعل التعرض كبيرًا لأي جهة تشغّله. والمقتطف الذي اطلعنا عليه لا يذكر رقم CVE ولا الإصدارات المتأثرة ولا التفاصيل التقنية للهجمات، لذا ينبغي التحقق منها في نشرة Broadcom الرسمية.

الخطوات المقترحة

على الجهات التي تشغّل vCenter Server التعامل مع التحديث كأولوية، والتأكد من الإصدارات المصححة في نشرة المورّد. وبما أن الاستغلال بدأ وفق التقرير قبل صدور الإصلاح بأشهر، فقد لا يكفي التحديث وحده، وينبغي فحص وجود مؤشرات اختراق سابقة. كما يُستحسن حصر الوصول إلى واجهات الإدارة في شبكات إدارية موثوقة إلى حين جدولة التحديث.

ما يجب فعله الآن

1. حصر جميع نسخ vCenter Server وتأكيد إصداراتها بالرجوع إلى نشرة Broadcom.
2. جدولة تحديث عاجل للنسخ المتأثرة باستخدام التحديثات الصادرة.
3. تقييد الوصول إلى واجهات إدارة vCenter بشبكات إدارية موثوقة.
4. مراجعة سجلات vCenter وحسابات المسؤولين بحثًا عن نشاط مشبوه منذ سبتمبر 2026.
5. الإبلاغ عن أي اختراق مؤكد عبر إجراءات الاستجابة للحوادث وإلى الجهة التنظيمية المختصة وفق المتطلبات.