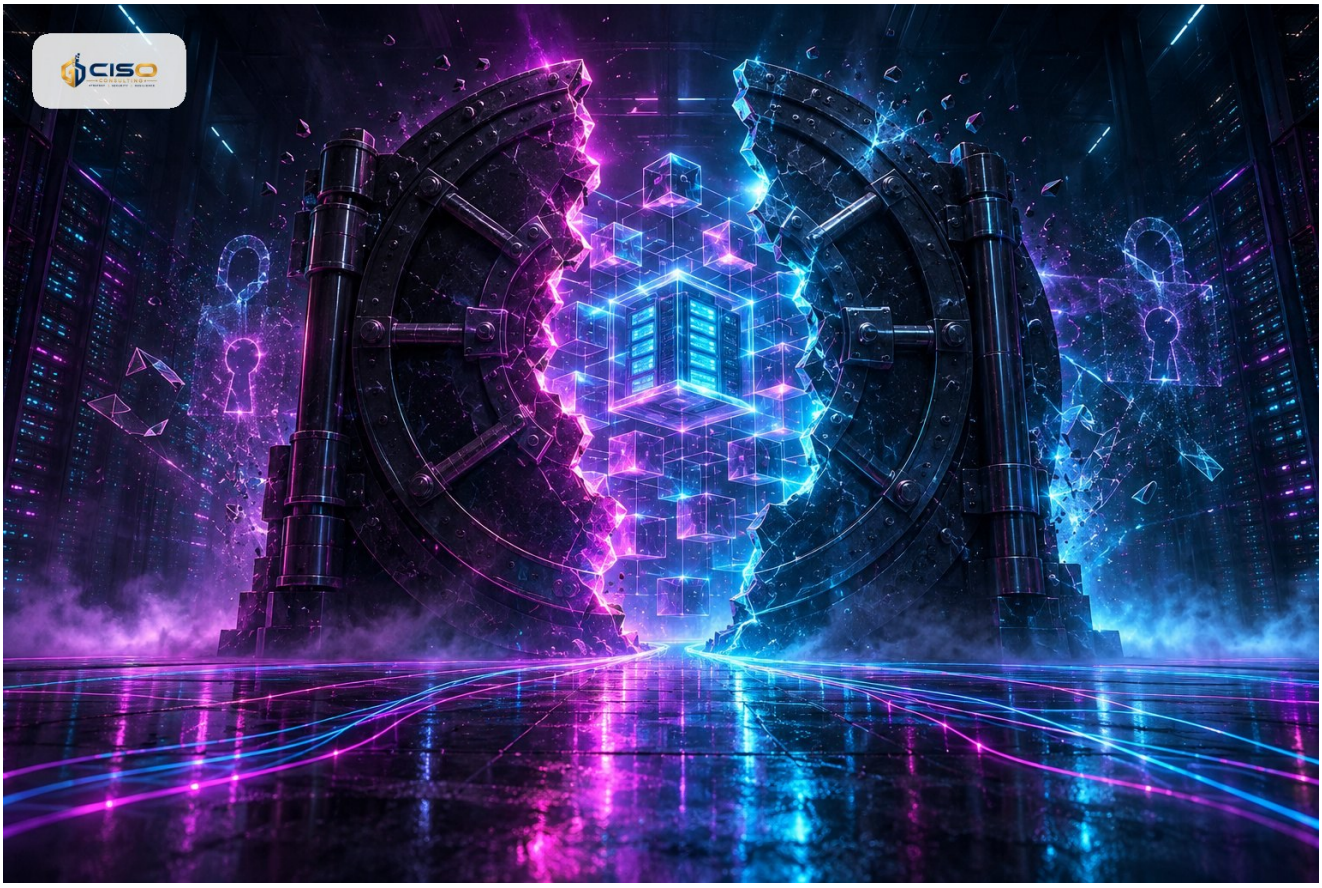
ثغرة حرجة في VMware vCenter (CVSS 9.8) تتيح تجاوز المصادقة عبر الشبكة



نشرت Broadcom نشرة أمنية عن ثغرة حرجة في vCenter تتيح لمهاجم لديه وصول إلى الشبكة تجاوز المصادقة. تتوفر إصدارات مُصححة لجميع الفروع المدعومة ولا يوجد حل بديل.

- الثغرة مصنفة بدرجة CVSS 9.8 وتؤثر في VMware vCenter.
- يمكن لمهاجم لديه وصول إلى الشبكة تجاوز المصادقة والحصول على وصول غير مصرح به.
- أعلنت عنها Broadcom، المالكة لـ VMware، في نشرة أمنية.
- تتوفر إصدارات مُصححة لجميع الفروع المدعومة.
- لا يذكر المورّد حلًا بديلًا، فالتحديث هو المعالجة الوحيدة.

نشرت Broadcom، المالكة لـ VMware، نشرة أمنية تصف ثغرة حرجة في VMware vCenter. تبلغ درجة الثغرة 9.8

وفق CVSS، وتتيح لمهاجم يستطيع الوصول إلى النظام عبر الشبكة تجاوز المصادقة والحصول على وصول غير مصرح به.

أهمية الأمر

يُعد vCenter الواجهة المركزية لإدارة مضيفات ESX والأجهزة الافتراضية في المنشأة. ولذلك فإن أي وصول غير مصرح به إليه يمس طبقة الإدارة في البيئة الافتراضية، وهو ما يستدعي التعامل مع النشرة كأولوية.

ما يذكره المورّد

صدرت إصدارات مُصححة لجميع الفروع المدعومة. ولا تذكر الشركة أي حل بديل، لذا يبقى تطبيق التحديث هو سبيل المعالجة. ولا يوضح المصدر ما إذا كانت الثغرة مستغلة فعلياً، ولا نقدّم أي ادعاء في هذا الشأن.

النهج الموصى به

ينبغي للفرق حصر نسخ vCenter لديها، وتأكيد الفرع والإصدار المستخدمين، وجدولة التحديث عبر إجراءات إدارة التغيير المعتادة بوتيرة معجّلة. وإلى حين التحديث، يخفف تقييد الوصول الشبكي إلى واجهة إدارة vCenter من التعرض، لكنه لا يغني عن التصحيح.

ما يجب فعله الآن

1. حصر جميع نسخ vCenter وتوثيق إصداراتها وفروعها.
2. مراجعة نشرة Broadcom لتحديد الإصدار المُصحح المناسب لكل فرع.
3. جدولة التحديث ضمن إجراء تغيير طارئ معجّل.
4. تقييد الوصول الشبكي إلى واجهات إدارة vCenter بشبكات الإدارة المصرح بها إلى حين التحديث.
5. مراجعة سجلات الوصول والمصادقة في vCenter بحثاً عن أي نشاط غير متوقع.