استغلال فعلي لثغرة تجاوز المصادقة في Xen Orchestra



حذّرت Vates VMS من ثغرة حرجة لتجاوز المصادقة في Xen Orchestra، تحمل المعرّف VSA-2026-062، ويجري استغلالها فعليًا. ولا يوجد لها معرّف CVE حتى الآن.

- أصدرت شركة Vates VMS الفرنسية التحذير الخاص بمنتج Xen Orchestra.
- الثغرة من نوع تجاوز المصادقة وتُتابَع تحت المعرّف VSA-2026-062.
- تفيد الشركة بأنها تُستغل فعليًا.
- لم يُخصَّص لها معرّف CVE بعد.
- يكمن الخلل في طريقة معالجة ملف تعريف الارتباط (cookie) لرمز المصادقة في واجهة REST.

حذّرت شركة Vates VMS من ثغرة حرجة في Xen Orchestra، منصة إدارة الافتراضية التي تقدمها، تفيد بأنها

تُستغل فعليًا. الثغرة من نوع تجاوز المصادقة وتحمل المعرّف VSA-2026-062، ولم يُخصَّص لها معرّف CVE حتى الآن.

ما تصفه الشركة

بحسب تنبيه الشركة، يقع الخلل في واجهة REST. إذ يُحوَّل رمز مصادقة مصوغ بطريقة خاصة داخل ملف تعريف الارتباط إلى كائن فارغ، ثم تمرره آلية المصادقة في REST إلى المرحلة التالية. ويتوقف المقتطف المتاح من المصدر عند هذه النقطة، لذلك لا نغطي هنا الآلية الكاملة ولا النتائج الدقيقة. ويشير عنوان الخبر إلى أن المهاجمين يستخدمون الثغرة للحصول على صلاحيات إدارية.

أهمية الأمر

تمتلك منصة إدارة البنية الافتراضية سيطرة واسعة على الأحمال التي تديرها. ولذلك فإن الوصول الإداري دون بيانات اعتماد صحيحة يمثل انكشافًا خطيرًا، كما أن الاستغلال الفعلي يعني أن التأجيل ليس خيارًا آمنًا. ولأنه لا يوجد CVE بعد، قد لا تُظهر الأدوات المعتمدة على قوائم CVE هذه الثغرة، فينبغي للفرق متابعة نشرة الشركة مباشرة.

لا يذكر المصدر الإصدارات المتأثرة ولا توفر تحديث تصحيحي. ينبغي الرجوع إلى نشرة Vates VMS لمعرفة هذه التفاصيل قبل اتخاذ الإجراء.

ما يجب فعله الآن

1. حصر جميع نسخ Xen Orchestra في بيئتكم، بما فيها نسخ الاختبار والنسخ المنسية.
2. الاطلاع على نشرة Vates VMS رقم VSA-2026-062 وتطبيق الإصلاح أو إجراء التخفيف الذي تحدده الشركة فور التأكد منه.
3. حصر الوصول إلى واجهة REST في Xen Orchestra ضمن شبكات الإدارة الموثوقة إلى حين اكتمال المعالجة.
4. مراجعة سجلات المصادقة والنشاط الإداري بحثًا عن جلسات إدارية غير متوقعة أو تغييرات غير مبررة.
5. تسجيل VSA-2026-062 يدويًا في سجل الثغرات لديكم لأنه لا يوجد CVE له بعد.