CISA تنبّه إلى ثغرة تجاوز المصادقة في Xen Orchestra ((CVE-2026-133469



أدرجت CISA الثغرة CVE-2026-133469 في Vates Xen Orchestra، إذ يمكن لمهاجم غير مصادَق تجاوز المصادقة والحصول على صلاحيات إدارية عبر رمز مصمَّم خصيصاً. يُنصح بتطبيق معالجات المورّد.

- CVE-2026-133469 ثغرة ناجمة عن ضعف التحقق من نوع المدخلات في Vates Xen Orchestra.
- يمكن لمهاجم غير مصادَق تجاوز المصادقة باستخدام رمز مصمَّم يحتوي على كائن JSON فارغ.
- يتيح الاستغلال الناجح تنفيذ إجراءات بصلاحيات إدارية.
- تطلب CISA تطبيق المعالجات وفق تعليمات المورّد، وحُدد 28-11-2026 موعداً للجهات الفيدرالية الأمريكية.
- إذا لم تتوفر معالجات، تفيد إرشادات CISA بالتوقف عن استخدام المنتج.

أضافت CISA الثغرة CVE-2026-133469 إلى قائمتها، وهي ناتجة عن ضعف في التحقق من نوع المدخلات في Vates Xen Orchestra. وقد تتيح لمهاجم غير مصادَق تجاوز المصادقة والعمل بصلاحيات إدارية.

ما ورد في المصدر

يشير الوصف إلى أن المهاجم يقدّم رمز مصادقة مصمَّماً خصيصاً يحتوي على كائن JSON فارغ، فلا يتحقق المنتج من نوع المدخل كما ينبغي ويمنح المهاجم صلاحيات المسؤول. ولا يتضمن المصدر تفاصيل تقنية إضافية.

وتتمثل الإجراءات التي تطلبها CISA في تطبيق المعالجات وفق تعليمات المورّد، والالتزام بإرشادات BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، إضافةً إلى متطلبات الفحص الجنائي الأولي (Forensics Triage Requirements). وفي الخدمات السحابية تُتَّبع إرشادات BOD 26-04 ذات الصلة. وإذا لم تتوفر معالجات فيجب التوقف عن استخدام المنتج. والموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026.

الخطوات المقترحة

تنطبق المهلة والتوجيهات رسمياً على الجهات الفيدرالية الأمريكية، لكنها مرجع مفيد لأي جهة تشغّل Xen Orchestra. وتقع على الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت، لذا يُنصح بحصر أماكن نشر المنتج ومعرفة ما إذا كانت واجهة الإدارة متاحة من الخارج.

ولأن الثغرة تفضي إلى وصول إداري، فينبغي إعطاء أولوية لأي نسخة معرّضة، والنظر في مراجعة جنائية بحثاً عن نشاط إداري غير مصرّح به بعد تطبيق المعالجات.

ما يجب فعله الآن

1. حصر جميع نسخ Vates Xen Orchestra وتحديد ما هو متاح منها عبر الإنترنت.
2. تطبيق معالجات المورّد في أقرب وقت، بدءاً بالنسخ المعرّضة للإنترنت.
3. التخطيط للتوقف عن استخدام أي نسخة لا تتوفر لها معالجة.
4. حصر الوصول إلى واجهة الإدارة في الشبكات الموثوقة فقط.
5. مراجعة سجلات النشاط الإداري على النسخ المتأثرة بحثاً عن إجراءات غير متوقعة، ورفع أي ملاحظات وفق إجراءات الاستجابة للحوادث.