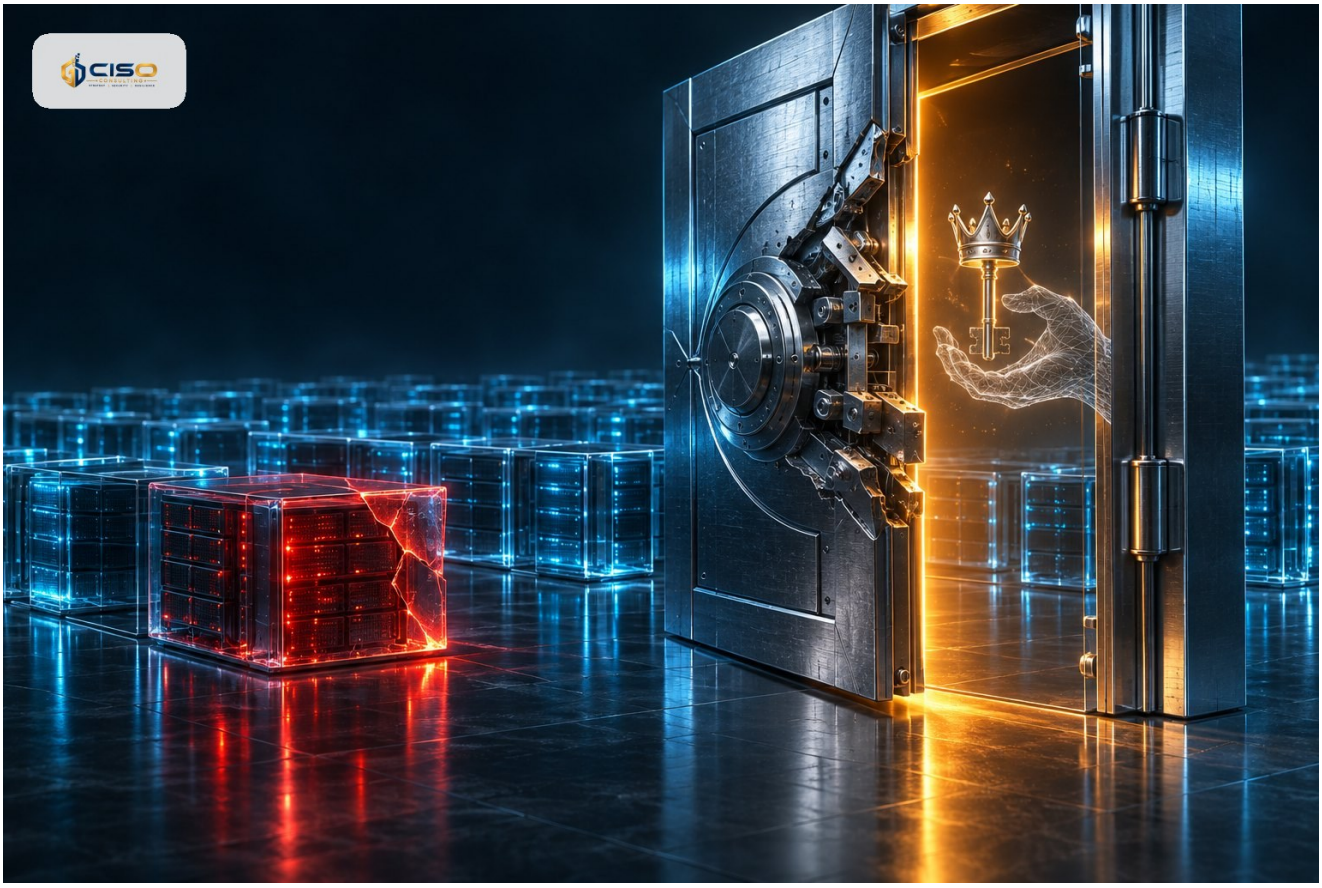
ثغرة حرجة لتجاوز المصادقة في Xen Orchestra تُستغل فعليًا في الهجمات



تُستغل حاليًا ثغرة حرجة لتجاوز المصادقة في Xen Orchestra، وقد تمنح المهاجم صلاحيات المسؤول والسيطرة على مضيفات الvirtualization من نوع XCP-ng.

- الثغرة من نوع تجاوز المصادقة وتصنَّف حرجة في Xen Orchestra.
- تفيد المصادر بأنها تُستغل فعليًا في هجمات قائمة.
- قد يؤدي الاستغلال الناجح إلى الحصول على صلاحيات المسؤول.
- يتيح ذلك السيطرة على مضيفات XCP-ng والأجهزة الافتراضية التي تعمل عليها.

ما الذي أُعلن

أفاد موقع BleepingComputer بأن ثغرة حرجة لتجاوز المصادقة في Xen Orchestra تُستغل حاليًا في هجمات

فعلية. وXen Orchestra منصة إدارة لبيئات الـ virtualization القائمة على XCP-ng. ووفق التقرير، يستطيع المهاجم الذي يستغل الثغرة الحصول على صلاحيات المسؤول والسيطرة على مضيفات XCP-ng.

لماذا يهم ذلك

تقع واجهة الإدارة فوق الأجهزة الافتراضية التي تتحكم بها، وإذا أمكن تجاوز مصادقتها فقد يصل المهاجم إلى جميع الأحمال التشغيلية على المضيفات المُدارة دون بيانات اعتماد صحيحة. وبما أن الاستغلال قائم بالفعل، ينبغي التعامل مع التعرض بوصفه خطرًا حاليًا لا نظريًا.

ولا يتضمن المقتطف المتاح من المصدر رقم CVE ولا أرقام الإصدارات المتأثرة ولا تفاصيل التصحيح، ولذلك يجب التحقق منها من نشرة المورّد مباشرة قبل التخطيط لأي تغيير.

الخطوات المقترحة

على الجهات التي تشغّل Xen Orchestra تحديد أماكن نشره ومن يستطيع الوصول إليه، ثم مراجعة نشرة المورّد الأمنية لمعرفة الإصدارات المصححة وتطبيقها عبر إجراءات التغيير الطارئ. وإلى حين ذلك، يُقيَّد الوصول الشبكي إلى واجهة الإدارة وتُراجع السجلات بحثًا عن نشاط إداري غير متوقع.

ما يجب فعله الآن

1. حصر جميع نسخ Xen Orchestra وتحديد ما يمكن الوصول إليه من شبكات غير موثوقة.
2. مراجعة نشرة المورّد الأمنية وتطبيق الإصدار المصحح عبر تغيير طارئ.
3. حصر الوصول إلى واجهة الإدارة في شبكات إدارية مخصصة أو عبر VPN.
4. مراجعة سجلات المصادقة ونشاط المسؤولين بحثًا عن دخول غير متوقع أو حسابات جديدة.
5. التأكد من سلامة النسخ الاحتياطية الحديثة للأجهزة الافتراضية الحرجة وحفظها بمعزل عن منصة الـ virtualization.