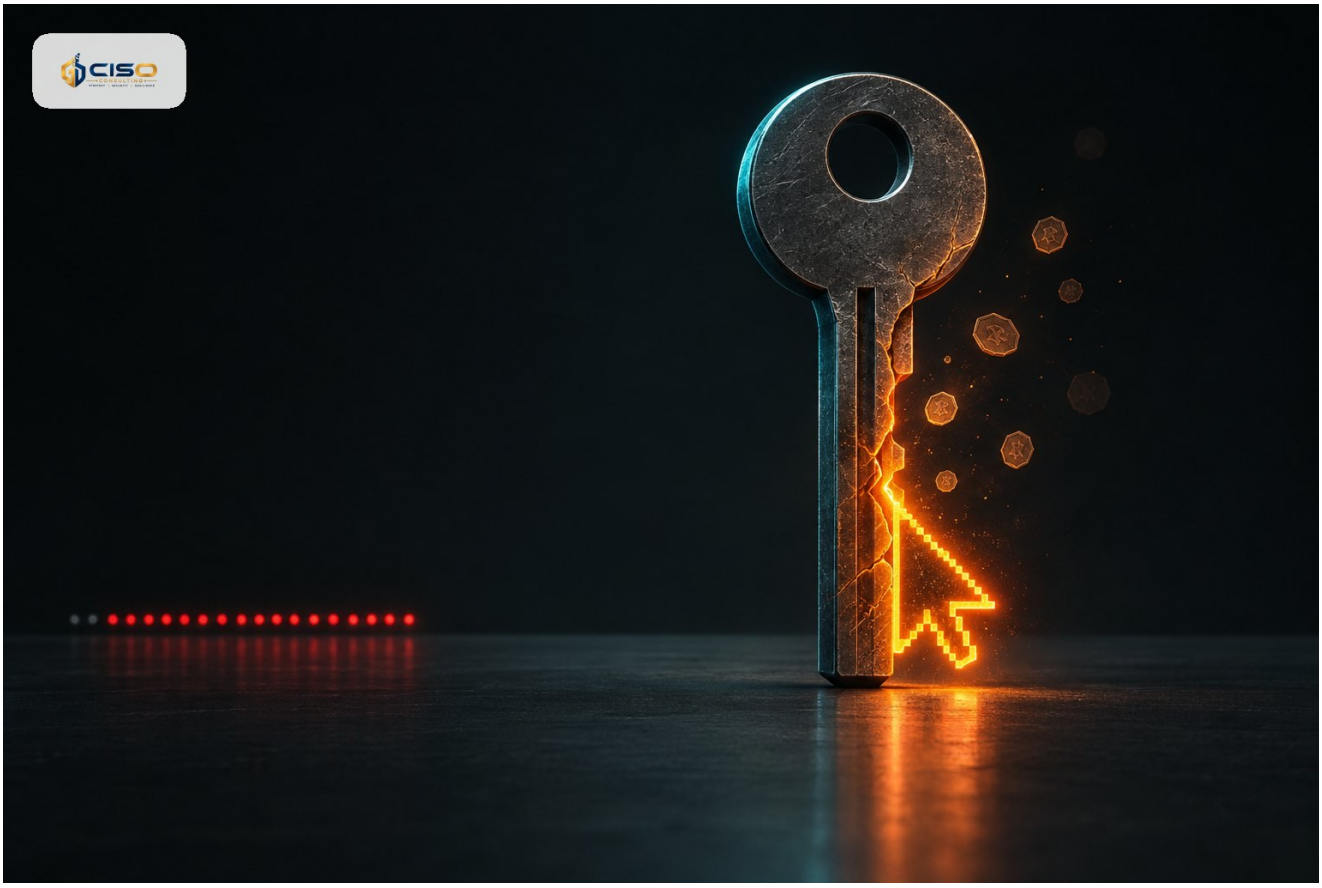
استغلال ثغرة "4EverAble2Shell" في N-able N-central خلال ساعات من نشر برهان المفهوم



يستغل مهاجمون ثغرة جديدة في N-central باسم 4EverAble2Shell للحصول على صلاحيات root وتثبيت برمجيات تعدين. أكد باحثون اختراق 21 خادماً، منها 19 على أحدث تحديث.

- تتيح 4EverAble2Shell لمهاجم غير مصادَق تنفيذ أوامر بصلاحيات root على خوادم N-central عند تفعيل Legacy API.
- تجمع سلسلة الهجوم بين ثغرة Apache Axis رقم CVE-2026-90436 وثغرة منفصلة لرفع الصلاحيات في N-central.
- أكدت Huntback اختراق 21 خادم N-central، منها 19 على الإصدار 2026.4.1.26 (Hotfix 2).
- الحمولات المرصودة تثبّت برنامج التعدين XMRig، لكن خوادم الإدارة عن بُعد المخترقة قد تُستخدم ضد عملاء المزوّد.
- عطّلت N-able تكامل Intune وتحث العملاء المحليين على إبقاء Legacy API معطّلًا.

ما الذي حدث

نشر الباحث Sean Bales أكواد برهان مفهوم لثغرتين جديدتين في N-central هما 4EverAble2Shell وAgent2Shell. بدأ استغلال الأولى في 12 نوفمبر بعد وقت قصير من النشر. وتُستخدم منصة N-central في المراقبة والإدارة عن بُعد (RMM) لدى مزوّدي الخدمات المُدارة وفرق تقنية المعلومات.

تتيح سلسلة 4EverAble2Shell لمهاجم غير مصادَق تنفيذ أوامر بصلاحيات root بشرط تفعيل Legacy API. وتستخدم ثغرة Apache Axis رقم CVE-2026-90436 لتنفيذ الأوامر بحساب الخدمة، ثم ثغرة منفصلة لرفع الصلاحيات حتى root. أما Agent2Shell فيُزعم أنها تتيح تنفيذ أوامر بصلاحيات SYSTEM على أجهزة Windows.

الاستغلال المرصود

رصدت Previdian وHuntback محاولات فحص على أنظمة الاستدراج عند نحو 08:30 بالتوقيت العالمي، تلتها محاولات لتنفيذ السلسلة كاملة. وعثرت Huntback على 21 خادم N-central مستضافاً يعمل عليها برنامج تعدين للمهاجم، منها 19 على الإصدار 2026.4.1.26 وهو Hotfix 2 الصادر في 10 نوفمبر. ثبّتت الحمولة برنامج XMRig لتعدين Monero مضبوطاً على استخدام نحو نصف أنوية المعالج.

الهجمات المرصودة حتى الآن تعدين خفي، غير أن الوصول بصلاحيات root إلى خادم RMM قد يتيح نشاطاً إضافياً ضد بيئات العملاء المُدارة.

استجابة المورّد

تقيّد N-able بعض الميزات والتكاملات، وعطّلت تكامل Intune، وتطلب من العملاء المحليين التأكد من تعطيل Legacy API وهو الوضع الافتراضي. كما تنصح بمواصلة ترقية Agents وProbes وفق إرشادات Hotfix 2. وذكرت في نشرتها أنها لم ترصد اختراقاً عبر الثغرات الجديدة، بينما أبلغ باحثون لاحقاً عن هجمات ناجحة.

ما يجب فعله الآن

1. حصر جميع نسخ N-central، بما فيها التي يديرها مزوّدو الخدمات نيابة عنكم، والتأكد من تعطيل Legacy API.
2. البحث في سجلات الويب عن الطلبات إلى /dms/services/ServerUI، خصوصاً التي تشير إلى jline.internal.TerminalLineSettings.
3. البحث عن خدمات systemd غير متوقعة باسم xvd.service وعمليات التعدين وملفات ضمن /tmp/.xvd/ أو /var/tmp/.xvd/.
4. اعتبار أي خادم تظهر عليه هذه المؤشرات مخترقاً بالكامل، ومراجعة الأجهزة المُدارة وبيانات الاعتماد التي كان يصل إليها.
5. مطالبة مزوّدي الخدمات المُدارة كتابياً بتوضيح تعرضهم والضوابط البديلة، وإبقاء Agents وProbes محدّثة وفق إرشادات N-able.