N-able تصدر تحديثات عاجلة لثغرات N-central المنشورة علنًا



أصدرت N-able التحديث N-central 2026.4 HF2 لمعالجة ثغرات صفرية نُشرت علنًا، وتحث عملاء النسخة المحلية على الترقية سريعًا. وترصد جهة استخبارات تهديدات عمليات فحص تستهدفها.

- يعالج N-central 2026.4 HF2 عددًا من الثغرات المسرّبة، ومنها ما تصفه N-able بأنه الأشد خطورة.
- تقول N-able إن جميع خوادم N-central المستضافة جرت ترقيتها، وتوصي عملاء النسخة المحلية بشدة بالترقية في أقرب وقت.
- ترصد Defused عمليات فحص، منها فتح جلسات وكيل مجهولة والوصول إلى نقطة التحكم عن بُعد دون مصادقة.
- تحصي Shadowserver نحو 148 خادم N-central مكشوفًا، بعد أن كان 1,338 يوم الاثنين.
- لم تصنّف N-able الثغرات بعد على أنها مستغلة فعليًا.

أصدرت N-able التحديث العاجل N-central 2026.4 HF2 لمعالجة ثغرات صفرية في منصة المراقبة والإدارة عن بُعد N-central. وكان باحث مستقل قد نشر الثغرات في 8 نوفمبر، فأوقفت N-able بيئاتها المستضافة احترازيًا ريثما تجهّز الإصلاحات.

ما الذي جرى إصلاحه

يعالج التحديث عددًا من الثغرات المنشورة، ومنها ما تصفه N-able بأنه الأشد خطورة. وتشمل ثغرات XXE وحقن OGNL (CVE-2026-125883 وCVE-2026-125878)، ورفع الصلاحيات محليًا (CVE-2026-125879 وCVE-2026-91000)، وXSS المخزّن (CVE-2026-125880)، وSSRF (CVE-2026-125881)، وتنفيذ الأوامر عن بُعد عبر اجتياز مسار رفع الملفات (CVE-2026-125882).

كما عرض الباحث سلسلة استغلال دون مصادقة قد تتيح لمهاجم تنفيذ أوامر على الخادم وإنشاء حساب مسؤول افتراضي غير مشروع. وتفيد N-able بأن الخوادم المستضافة جرت ترقيتها، وتوصي بشدة عملاء النسخة المحلية بالترقية في أقرب وقت واتباع إرشاداتها المنشورة قبل استعادة الوصول الاعتيادي.

مستوى التعرض الحالي

لم تصنّف N-able الثغرات بعد على أنها مستغلة. غير أن Defused رصدت خلال 24 ساعة عمليات فحص شملت جلسات وكيل مجهولة وسحب إعدادات الجهاز وطلبات إلى نقطة التحكم عن بُعد دون مصادقة. وتشير Shadowserver إلى نحو 148 خادمًا مكشوفًا، بعد أن كان 1,338 يوم الاثنين.

ولأن N-central تدير شبكات العملاء وأجهزتهم من لوحة واحدة، ينبغي للجهات التي تشغّلها بنفسها أو تعتمد على مزوّد يستخدمها التعامل مع هذا التحديث كأولوية.

ما يجب فعله الآن

1. حدّدوا ما إذا كانت N-central مستخدمة داخليًا أو لدى أي مزوّد خدمات مُدارة لديه وصول إلى بيئتكم.
2. رقّوا N-central المحلية إلى 2026.4 HF2 وفق إرشادات N-able المنشورة قبل استعادة الوصول.
3. تأكدوا من عدم إمكانية الوصول إلى خوادم N-central من الإنترنت، وقيّدوا الإدارة بشبكات موثوقة أو VPN.
4. راجعوا سجلات N-central بحثًا عن جلسات وكيل مجهولة أو حسابات Default Administrator غير متوقعة أو طلبات تحكم عن بُعد دون مصادقة.
5. أعيدوا تعيين بيانات اعتماد مسؤولي N-central وراجعوا الحسابات عند ظهور نشاط مشبوه.
6. اطلبوا من مزوّدي الخدمات المُدارة تأكيد حالة التحديث والإبلاغ عن أي اشتباه باختراق.