# N-able تحقق في ادعاءات جديدة عن ثغرات في N-central المحلي



تحقق N-able في إفصاح علني يزعم وجود ثغرات إضافية في N-central المحلي، منها الإصدار 2026.4.1 HF2. وتربط مراجعتها الأولية المشكلة بإعداد غير افتراضي: تفعيل Legacy API وإتاحته على الإنترنت.

- أعلنت N-able أنها تحقق في إفصاح علني جديد يتضمن ادعاءات بثغرات إضافية في N-central المحلي.
- تتعلق الادعاءات بالإصدار 2026.4.1 HF2.
- يشير عنوان الخبر إلى تنفيذ أوامر عن بُعد بصلاحيات root وإلى وصول بصلاحيات SYSTEM في Windows، وإلى أن الاستغلال ينجح ضد خوادم مُحدّثة.
- تفيد مراجعة N-able الأولية بأن مشكلة الخادم تعتمد على تفعيل Legacy API وإتاحته على الإنترنت، وهو ليس الإعداد الافتراضي.

## ما الذي أُعلن

ذكرت N-able يوم الخميس أنها تدرس إفصاحًا علنيًا جديدًا يتضمن ادعاءات بوجود ثغرات إضافية في خوادم N-central المحلية العاملة بالإصدار 2026.4.1 HF2. وبحسب عنوان الخبر، تنجح هذه الاستغلالات ضد خوادم مُحدّثة بالفعل، ويمكن أن تتيح تنفيذ أوامر عن بُعد بصلاحيات root ووصولاً بصلاحيات SYSTEM في Windows.

## ما تقوله N-able حتى الآن

تصف N-able تقييمها في النشرة بأنه مراجعة أولية. وعلى هذا الأساس، تعتمد مشكلة الخادم على إعداد غير افتراضي يكون فيه **Legacy API** مفعّلاً ومتاحًا من الإنترنت العام. ولا يقدّم المقتطف المتاح تفاصيل تقنية أخرى، ولا نطاقًا للإصدارات المتأثرة غير المذكور، ولا جدولاً زمنيًا للمعالجة، وتبقى هذه النقاط مفتوحة.

## لماذا يهم ذلك

تُعد N-central منصة للمراقبة والإدارة عن بُعد، والخادم المحلي منها يملك عادةً وصولاً مميزًا إلى البيئات المُدارة. لذا ينبغي للمؤسسات التي تشغّلها أخذ الادعاءات بجدية أثناء استمرار تحقيق المورّد، دون افتراض أن التعرض ينطبق على كل نشر. ويوفّر الشرط الذي ذكرته N-able فحصًا أوليًا عمليًا: هل Legacy API مفعّل، وهل يمكن الوصول إليه من الخارج.

إلى أن تنشر N-able مزيدًا من المعلومات، يكون النهج المناسب هو التحقق من تعرّضكم، وتقليصه حيثما أمكن، ومتابعة نشرة المورّد.

## ما يجب فعله الآن

1. حصر جميع خوادم N-central المحلية والتحقق من الإصدار المستخدم، ومنه ما إذا كان 2026.4.1 HF2.
2. التحقق مما إذا كان Legacy API مفعّلاً وما إذا كان يمكن الوصول إليه من الإنترنت العام.
3. تعطيل Legacy API إن لم تكن هناك حاجة إليه، أو حصر الوصول إليه في الشبكات الداخلية الموثوقة أو VPN فقط.
4. مراجعة سجلات خادم N-central وواجهة API بحثًا عن وصول أو نشاط غير متوقع، وتصعيد أي اشتباه عبر إجراءات الاستجابة للحوادث.
5. متابعة نشرة N-able وتطبيق التوجيهات أو التحديثات فور صدورها.
6. إبلاغ فريقي مخاطر الأطراف الخارجية ومركز العمليات الأمنية، والنظر في التزامات الإبلاغ للجهة المنظمة عند ثبوت اختراق.