شركة N-able توقف بيئات N-central المستضافة بعد الكشف العلني عن أكثر من 30 ثغرة



أوقفت N-able بيئات N-central المستضافة، وطلبت من عملائها الذين يديرون الخوادم محلياً إيقافها حتى إشعار آخر، بعد الإفصاح العلني عن أكثر من 30 ثغرة مجمّعة تحت اسم Able2Shell.

- أوقفت N-able بيئات N-central المستضافة مؤقتاً كإجراء احترازي.
- تحثّ الشركة العملاء الذين يشغّلون N-central محلياً على إيقاف خوادمهم حتى إشعار آخر.
- السبب هو الإفصاح العلني عن أكثر من 30 ثغرة مجمّعة تحت اسم Able2Shell.
- يشير عنوان الخبر إلى 33 ثغرة يوم صفر مع شيفرات استغلال تجريبية نشرها باحث.
- تقول N-able إنها تتخذ الإجراءات اللازمة لتأمين البيئة.

أعلنت N-able أنها توقف مؤقتاً بيئات N-central المستضافة كإجراء احترازي ريثما تؤمّنها، كما تحثّ العملاء الذين

يشغّلون N-central داخل منشآتهم على إيقاف خوادمهم حتى إشعار آخر.

ما الذي حدث

جاء هذا الإجراء بعد الإفصاح العلني عن أكثر من 30 ثغرة مجمّعة تحت اسم **Able2Shell**. وبحسب عنوان المصدر، كشف باحث عن 33 ثغرة يوم صفر مصحوبة بشيفرات استغلال تجريبية. ولا يتضمن المقتطف المتاح أرقام CVE أو تفاصيل تقنية أو تأكيداً لوقوع استغلال فعلي، ولذلك لا نفترض شيئاً في هذه النقاط.

لماذا يهم ذلك

تُعد N-central منصة للمراقبة والإدارة عن بُعد، وهذه المنصات تتمتع عادةً بصلاحيات واسعة على عدد كبير من الأجهزة المُدارة. لذلك يستحق طلب الإيقاف من المورّد اهتمام أي جهة تستخدم المنصة مباشرة أو عبر مزوّد خدمات مُدارة. كما أن توافر شيفرات استغلال تجريبية علنية يقصّر عادةً المدة قبل أن يحاول المهاجمون استغلال الثغرات.

الخطوات التالية

تابعوا تعليمات N-able وتحديثاتها، واعتبروا طلب إيقاف الخوادم المحلية هو التوجيه الحالي. وتحققوا مما إذا كانت فرقكم أو مزوّدو الخدمة لديكم يستخدمون N-central، واستعدوا لفترة قد تتعطل فيها أدوات الإدارة عن بُعد.

ما يجب فعله الآن

1. حصر جميع نسخ N-central، المستضافة والمحلية، لديكم ولدى مزوّدي الخدمات المُدارة.
2. إيقاف خوادم N-central المحلية كما طلبت N-able إلى حين صدور توجيهات إضافية.
3. مطالبة مزوّدي الخدمات المُدارة كتابياً بالإفادة عن استخدامهم N-central والضوابط المؤقتة المطبقة.
4. تجهيز مسارات بديلة ومضبوطة للدعم عن بُعد العاجل خلال توقف المنصة.
5. مراجعة النشاط الإداري الأخير في N-central والحسابات وبيانات الاعتماد المرتبطة بها، وتصعيد أي نشاط مريب عبر مسار الاستجابة للحوادث.
6. متابعة بيانات N-able الرسمية وتطبيق توجيهاتها فور صدورها.