CISA تدرج ثغرة مستغلة في N-able Mail Assure بينما تعيد الشركة الخدمة



أضافت CISA الثغرة CVE-2026-134624 في N-able Mail Assure بدرجة 9.3 إلى قائمة الثغرات المستغلة. وتقول N-able إنها عالجتها ولم تجد استغلالاً إلا على خادم واحد تستضيفه.

- الثغرة CVE-2026-134624 تؤثر في منصة أمن البريد N-able Mail Assure وتبلغ درجة خطورتها 9.3.
- أدرجتها CISA في قائمة الثغرات المستغلة وحددت للجهات الاتحادية الأمريكية مهلة حتى عيد الشكر.
- اخترق مهاجمون خادمًا واحدًا تستضيفه N-able عبر الثغرة، مما عطّل خدمتي Mail Assure وSpamExperts نحو أسبوع.
- تفيد N-able بأن تدفق البريد وتصفية الرسائل المزعجة استمرا، ولم تجد استغلالاً خارج ذلك الخادم.

- وعدت الشركة بنشر تحليل للسبب الجذري خلال أسبوعين، وتقول إن الحادث غير مرتبط بثغرات N-central الأخيرة.

أدرجت CISA الثغرة CVE-2026-134624 في منصة أمن البريد N-able Mail Assure ضمن قائمتها للثغرات المستغلة. وتبلغ درجة خطورة الثغرة 9.3، وطُلب من الجهات الاتحادية الأمريكية معالجتها قبل عيد الشكر.

ما الذي حدث

وفق التقرير، استغل مهاجمون الثغرة لاختراق خادم واحد تستضيفه N-able، فأدى ذلك إلى انقطاعات استمرت نحو أسبوع وطالت خدمتي Mail Assure وSpamExpertsg. وأبلغت N-able موقع Recorded Future News بأنها عالجت الثغرة خلال عطلة نهاية الأسبوع وأعادت وصول العملاء إلى لوحات المتابعة الداخلية. وتؤكد أن البريد الوارد والصادر وتصفية الرسائل المزعجة ظلت تعمل طوال الحادث.

وتذكر الشركة أن المسح والمراقبة المستمرين لم يكشفا استغلالاً خارج الخادم الذي حُدد في بداية التحقيق، وأنها استعانت بفرق استجابة للحوادث للتحقق من ذلك. ووعدت بنشر تحليل للسبب الجذري خلال أسبوعين.

مشكلات أخرى مرتبطة بالشركة

تقول N-able إن الحادث غير مرتبط بأكثر من 30 ثغرة في منصة الإدارة عن بعد N-central كشف عنها باحث قبل أسبوعين. وفي تلك الحالة أوقفت الشركة بيئات N-central المستضافة وطلبت من العملاء إيقاف خوادمهم. ويشير التقرير أيضًا إلى أن ثغرة في N-central استُخدمت في هجوم على سلسلة التوريد بالفدية في أغسطس.

الأهمية

تتمتع خدمات أمن البريد وأدوات الإدارة عن بعد بصلاحيات واسعة داخل بيئة المؤسسة. وعلى الجهات التي تستخدم منتجات N-able مباشرة أو عبر مزود خدمات مُدارة أن تتحقق من تعرضها وتطلب ضمانات مكتوبة بدل الاكتفاء بالبيانات العلنية.

ما يجب فعله الآن

1. حدد ما إذا كانت Mail Assure أو SpamExperts أو N-central مستخدمة لديكم، بما في ذلك عبر مزودي الخدمات المُدارة.
2. اطلب من N-able أو من مزودكم تأكيدًا كتابيًا بحالة المعالجة وما إذا كانت بيئتكم قد تأثرت.
3. راجع سجلات بوابة البريد والسجلات الإدارية بحثًا عن نشاط غير معتاد أو تغييرات غير متوقعة في الإعدادات.
4. غيّر بيانات الاعتماد ومفاتيح الواجهات البرمجية المرتبطة بالخدمات المتأثرة إذا لم يستطع المزود استبعاد تعرضها.
5. تابع تحليل السبب الجذري الموعود وحدّث تقييم مخاطر الأطراف الثالثة وفقًا له.
6. التزم بمتطلبات الإبلاغ عن الحوادث للجهة التنظيمية المعنية في حال تأكد التأثر.