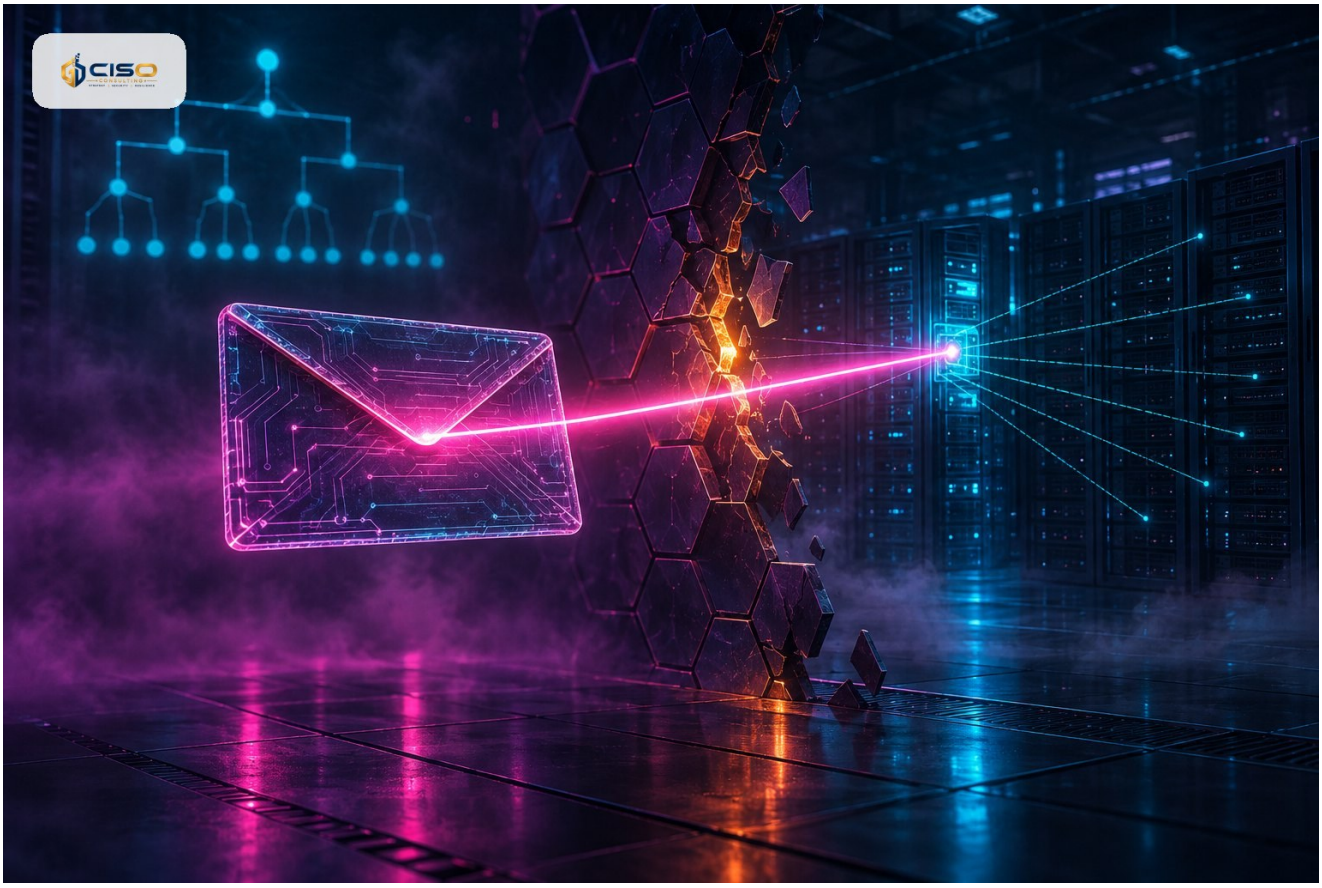
ثغرة SSRF في N-able MailAssure (CVE-2026-134624): طبّقوا معالجات المورّد



أدرجت CISA الثغرة CVE-2026-134624 وهي من نوع SSRF في فحص مزامنة LDAP بمنتج N-able MailAssure (SpamExperts)، وتتيح لمستخدم API موثّق استكشاف أجهزة ومنافذ داخلية وإرسال بيانات مصاغة إلى خدمات داخلية.

- الثغرة من نوع تزوير الطلبات من جهة الخادم (SSRF) في فحص اتصال مزامنة LDAP بمنتج N-able MailAssure (SpamExperts).
- يستطيع مستخدم API موثّق الاتصال بأجهزة ومنافذ داخلية عشوائية ومعرفة المتاح منها.
- يمكنه أيضاً إرسال بيانات مصاغة خصيصاً إلى خدمات داخلية.
- تشترط CISA تطبيق المعالجات وفق تعليمات المورّد، بما يتوافق مع BOD 26-04 ومتطلبات الفرز الجنائي.
- إن لم تتوفر معالجات تدعو CISA إلى التوقف عن استخدام المنتج، والموعد الاتحادي هو

.26-11-2026

أضافت CISA الثغرة CVE-2026-134624 إلى قائمتها. وهي ثغرة تزوير طلبات من جهة الخادم (SSRF) في منتج N-able MailAssure (SpamExperts)، وتقع في فحص الاتصال المستخدم لمزامنة LDAP.

ما الذي تتيحه الثغرة

يستطيع مستخدم API موثّق دفع المنتج إلى الاتصال بأجهزة ومنافذ داخلية عشوائية، وبذلك يعرف الأنظمة الداخلية التي يمكن الوصول إليها، ويرسل بيانات مصاغة خصيصاً إلى خدمات داخلية. ولا يذكر المصدر تفاصيل استغلال محددة ولا الإصدارات المتأثرة.

ما تطلبه CISA

الإجراء المطلوب هو تطبيق المعالجات وفق تعليمات المورّد، بما ينسجم مع توجيه BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر ومع متطلبات الفرز الجنائي. وإذا لم تتوفر معالجات، فيُتبع توجيه BOD 26-04 الخاص بالخدمات السحابية أو يُتوقف عن استخدام المنتج. وعلى الجهات تقييم تعرّض كل أصل للإنترنت بنفسها. والموعد الاتحادي هو 26-11-2026.

الصلة بالجهات في المملكة

يُلزم BOD 26-04 الجهات الاتحادية الأمريكية، لكن الانضباط نفسه يناسب الجهات المنظمة في المملكة التي تشغّل MailAssure. وبما أن الاستغلال يتطلب مستخدم API موثّقاً، فإن الوصول إلى واجهة API وبيانات الاعتماد المرتبطة بها يستحق الاهتمام إلى جانب التحديث.

ما يجب فعله الآن

1. حدّدوا ما إذا كان N-able MailAssure (SpamExperts) مستخدماً في بيئتكم، بما في ذلك عبر الخدمات المُدارة أو السحابية.
2. طبّقوا معالجات المورّد ووثّقوا تاريخ التغيير ونطاقه.
3. راجعوا من يملك بيانات اعتماد API، واحذفوا الحسابات غير الضرورية وبدّلوا بيانات الباقي.
4. افحصوا سجلات API والخادم بحثاً عن فحوص اتصال مزامنة LDAP موجهة إلى أجهزة أو منافذ داخلية غير متوقعة.
5. إذا لم تتوفر معالجات، فخطّطوا للتوقف عن استخدام المنتج كما تنصح CISA، ودوّنوا القرار في سجل المخاطر.