N-able تصلح ثغرة SSRF حرجة اكتُشفت أثناء التحقيق في هجوم Mail Assure



أصلحت N-able الثغرة (CVSS 9.3) CVE-2026-134624 من نوع SSRF التي اكتُشفت أثناء التحقيق في الهجوم على Mail Assure وSpamExperts. على العملاء التأكد من الإصدار المصحَّح ومراجعة بيانات الاعتماد.

- CVE-2026-134624 ثغرة SSRF بتقييم CVSS 9.3، أُصلحت في إصدار Mail Assure/SpamExperts رقم 20261121.1943.
- تتيح الثغرة لمستخدم API يملك صلاحيات كافية دفع الخادم إلى الاتصال بمضيفات ومنافذ داخلية عشوائية وإرسال بيانات مصمَّمة إليها.
- استهدف الهجوم السابق خادم ويب وربما وصل إلى بيانات اعتماد مخزّنة فيه؛ وغيّرت N-able بيانات الاعتماد وألغت رموز API وOAuth.
- تفيد N-able بأن الاستغلال اقتصر على خادم واحد تستضيفه، ولم ترصد المراقبة اللاحقة نشاطًا

خبيثًا.

- وعدت الشركة بتحليل رسمي للسبب الجذري خلال أسبوعين.

أصلحت N-able ثغرة حرجة من نوع تزوير الطلبات من جهة الخادم (SSRF) تحمل الرقم CVE-2026-134624 وبتقييم CVSS يبلغ 9.3. وقد اكتُشفت الثغرة أثناء تحقيق الشركة في هجوم سيبراني استهدف خدمتي Mail Assure وSpamExperts Hosted Cloud.

ما الذي حدث

في 16 نوفمبر عطّلت N-able الوصول إلى البوابة وواجهة API وعلّقت خدمات مرتبطة بها، منها السجلات ومزامنة صناديق البريد وبوابة الإدارة والحجر الصحي، دون أن يتأثر تسليم البريد. ثم أكدت الشركة وقوع هجوم أصاب خادم ويب، وأن المهاجمين وصلوا على الأرجح إلى بعض بيانات الاعتماد المخزّنة عليه.

احتوت الشركة الحادث، وغيّرت بيانات الاعتماد، وألغت رموز API وOAuth. وأعادت الوصول إلى لوحة التحكم وواجهات API في 21 نوفمبر مع استمرار المراقبة.

الثغرة

لم تكن الخدمة تقيّد وجهة اختبار اتصال مزامنة LDAP الذي يُجرى عند إعداد الترحيل. ولذلك كان بإمكان مستخدم API يملك صلاحيات كافية أن يجعل الخادم يتصل بمضيفات ومنافذ داخلية عشوائية، ويحدد المتاح منها، ويرسل بيانات مصمَّمة إلى خدمات داخلية. ويتضمن الإصدار 20261121.1943 الإصلاح.

وتذكر N-able أن الاستغلال اقتصر على خادم واحد تستضيفه، وأن المراقبة منذ المعالجة لم تكشف نشاطًا خبيثًا إضافيًا. ويتواصل التحقيق، ومن المتوقع صدور تحليل رسمي للسبب الجذري خلال أسبوعين.

لماذا يهم ذلك

على الجهات التي تستخدم هذه الخدمات لتصفية البريد التعامل مع الأمر بوصفه حادثًا لدى مورّد: التحقق من مدى تأثرها، ومراجعة بيانات الاعتماد والرموز المرتبطة بالخدمة، ومتابعة تحليل السبب الجذري المرتقب.

ما يجب فعله الآن

1. تأكدوا مع N-able من أن بيئتكم تعمل بإصدار Mail Assure/SpamExperts رقم 20261121.1943 أو أحدث.
2. غيّروا بيانات الاعتماد ومفاتيح API ورموز OAuth المرتبطة بالخدمة، حتى لو ألغت N-able رموزها من جانبها.
3. راجعوا المستخدمين الذين يملكون صلاحيات API على الخدمة واسحبوا ما لا حاجة إليه.
4. افحصوا السجلات بحثًا عن نشاط غير معتاد في API أو مزامنة LDAP وعن اتصالات داخلية غير متوقعة من الخدمة.
5. وثّقوا الحدث ضمن إجراءات إدارة حوادث الأطراف الثالثة، واطلبوا من N-able تحليل السبب الجذري عند صدوره.