CISA تضيف ثغرتين في MONAI Label وN-able Mail Assure إلى قائمة الثغرات المستغلة



أضافت CISA ثغرتين إلى كتالوج KEV لوجود أدلة على استغلالهما فعليًا: ثغرة اجتياز مسار في MONAI Label وثغرة SSRF في N-able Mail Assure (SpamExperts). يُنصح بالتحقق من استخدامهما.

- الثغرة CVE-2026-133968 هي ثغرة اجتياز مسار (Path Traversal) في MONAI Label من Project MONAI.
- الثغرة CVE-2026-134624 هي ثغرة تزوير طلبات من جهة الخادم (SSRF) في N-able Mail Assure (SpamExperts).
- أُضيفت الثغرتان إلى كتالوج KEV استنادًا إلى أدلة على استغلال فعلي.
- تصف CISA هذين النوعين من الثغرات بأنهما وسيلة هجوم متكررة لدى الجهات الخبيثة.
- التوجيه BOD 26-04 ملزم للجهات الفيدرالية المدنية الأمريكية فقط، لكن CISA تشجع جميع

> المؤسسات على إعطاء الأولوية لثغرات KEV.

أضافت CISA ثغرتين إلى كتالوج الثغرات المستغلة المعروفة (KEV) بعد رصد أدلة على استغلالهما فعليًا.

ما الذي أُضيف

- **CVE-2026-133968**: ثغرة اجتياز مسار (Path Traversal) في MONAI Label من Project MONAI.
- **CVE-2026-134624**: ثغرة تزوير طلبات من جهة الخادم (SSRF) في N-able Mail Assure (SpamExperts).

وتشير CISA إلى أن هذين النوعين من الثغرات يمثلان وسيلة هجوم متكررة لدى الجهات الخبيثة. ولا يتضمن المصدر الإصدارات المتأثرة ولا تفاصيل التصحيح ولا هوية الجهات المستغِلة، لذا يُرجع إلى نشرات الموردين للحصول عليها.

أهمية الخبر خارج الولايات المتحدة

يُلزم التوجيه التشغيلي BOD 26-04 الجهات الفيدرالية المدنية الأمريكية بمعالجة ثغرات KEV سريعًا، لا سيما على الأصول المكشوفة للإنترنت التي يمنح استغلالها سيطرة كاملة، ويحدد كذلك توقعات للتحقق مما إذا كان النظام قد اختُرق قبل تطبيق التصحيح. ولا ينطبق التوجيه على غير تلك الجهات، لكن CISA تشجع جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء أولوية لمعالجة ثغرات الكتالوج.

والخطوة العملية للمؤسسات في المملكة محدودة: تأكدوا مما إذا كان أي من المنتجين موجودًا في بيئتكم، بما في ذلك لدى مزودي الخدمات المُدارة، وتعاملوا مع أي تطابق كبند ذي أولوية في قائمة التحديثات.

الخطوات التالية

تساعد الإجراءات أدناه في تأكيد التعرض وتطبيق إصلاحات الموردين والبحث عن مؤشرات اختراق سابق.

ما يجب فعله الآن

1. ابحثوا في سجل الأصول وعقود مزودي الخدمة عن MONAI Label وN-able Mail Assure (SpamExperts).
2. راجعوا نشرات الموردين وطبقوا الإصلاحات أو إجراءات التخفيف المتاحة، بدءًا بالنسخ المكشوفة للإنترنت.
3. افحصوا السجلات والأنظمة بحثًا عن مؤشرات اختراق سابقة لتطبيق التصحيح.
4. أدرجوا مدخلات كتالوج KEV ضمن فرز الثغرات بوصفها أولوية عالية.
5. اطلبوا من مزودي الخدمات المُدارة تأكيد ما إذا كانوا يستخدمون أيًا من المنتجين نيابةً عنكم.