CISA تحذّر من ثغرة اجتياز مسار في MONAI Label التابع لـ Project MONAI (CVE-2026-133968)



أدرجت CISA الثغرة CVE-2026-133968 في MONAI Label، وهي اجتياز مسار يتيح لمهاجم عن بُعد دون مصادقة كتابة ملفات خارج مجلد البيانات، وقد يقود إلى تنفيذ تعليمات عن بُعد.

- الثغرة من نوع اجتياز مسار في MONAI Label التابع لـ Project MONAI.
- يستطيع مهاجم عن بُعد دون مصادقة كتابة ملفات عشوائية خارج مجلد البيانات المقصود.
- قد يؤدي الاستغلال الناجح إلى تنفيذ تعليمات عن بُعد.
- تشترط CISA تطبيق المعالجات وفق تعليمات المورّد وتوجيه BOD 26-04 ومتطلبات الفرز الجنائي الرقمي.
- إذا لم تتوفر معالجة، توصي CISA بالتوقف عن استخدام المنتج؛ والموعد النهائي للجهات الفيدرالية الأمريكية هو 26-11-2026.

أضافت CISA الثغرة CVE-2026-133968 إلى قائمة الثغرات التي تتطلب إجراءً. وتؤثر الثغرة في MONAI Label، وهو جزء من Project MONAI، وهي من نوع اجتياز المسار.

ما الذي تتيحه الثغرة

يستطيع مهاجم لديه وصول شبكي ودون مصادقة كتابة ملفات عشوائية خارج المجلد المخصص لتخزين بيانات MONAI Label. ولأن المهاجم يستطيع وضع ملفات في مواقع لا ينبغي للتطبيق الوصول إليها، فقد يقود ذلك إلى تنفيذ تعليمات عن بُعد على النظام المتأثر.

ما تطلبه CISA

توجّه CISA الجهات إلى تطبيق المعالجات وفق تعليمات المورّد، وبما يتوافق مع توجيه BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، ومع متطلبات الفرز الجنائي الرقمي (Forensics Triage Requirements). وفي حالة الخدمات السحابية يُتَّبع توجيه BOD 26-04 ذي الصلة. وإذا لم تتوفر معالجات فتوصي CISA بالتوقف عن استخدام المنتج. وعلى الجهات تقييم تعرّض كل أصل للإنترنت بنفسها. والموعد النهائي للجهات الفيدرالية الأمريكية هو 26-11-2026، وهو ملزم لها وحدها لكنه مرجع مفيد لغيرها.

قراءة عملية

لا يذكر المصدر تفاصيل عن استغلال فعلي ولا الإصدارات المتأثرة، لذا ينبغي الرجوع إلى تعليمات المورّد لمعرفة النطاق والإصلاحات. وعلى الجهات التي تستخدم MONAI Label، كما في بيئات التصوير الطبي أو البحث، تحديد أماكن تشغيله ومعرفة ما إذا كان يمكن الوصول إليه من خارج الشبكة.

ما يجب فعله الآن

1. حصر جميع نسخ MONAI Label المنشورة، بما فيها بيئات البحث والاختبار.
2. التحقق من إمكانية الوصول إلى كل نسخة من الإنترنت وتقييد الوصول إليها حتى تتم المعالجة.
3. تطبيق معالجات المورّد، وإذا لم تتوفر فالتخطيط للتوقف عن استخدام المنتج.
4. فحص الخوادم المتأثرة بحثًا عن ملفات غير متوقعة كُتبت خارج مجلد البيانات، مع حفظ الأدلة للفرز الجنائي الرقمي.
5. تسجيل الثغرة وخطة المعالجة في سجل المخاطر وإجراءات إدارة الثغرات.