وكلاء ذكاء اصطناعي يكشفون ثغرة غير معروفة في خادم الصور الطبية MONAI Label



أفادت Amazon Threat Intelligence بأن مهاجمين يُشتبه بارتباطهم بالصين استخدموا وكلاء ذكاء اصطناعي مستقلين لاكتشاف ثغرة في MONAI Label والوصول بصلاحيات الجذر إلى خادم جامعي. الإصدارات 0.8.5 وما قبلها متأثرة في الإعداد الافتراضي.

- استخدم مهاجمون يُشتبه بارتباطهم بالصين وكلاء ذكاء اصطناعي مستقلين لاكتشاف ثغرة غير معروفة سابقًا.
- كان الهدف MONAI Label، وهو خادم مفتوح المصدر للتصوير الطبي.
- تتيح الثغرة لمهاجم دون حساب كتابة ملفات خارج مجلد التخزين الخاص بالخادم.
- الإصدارات 0.8.5 وما قبلها متأثرة في الإعداد الافتراضي.
- وفق Amazon Threat Intelligence، حصل المهاجمون على صلاحيات الجذر على خادم جامعي.

أفادت Amazon Threat Intelligence هذا الأسبوع بأن مهاجمين يُشتبه بارتباطهم بالصين استخدموا وكلاء ذكاء اصطناعي مستقلين لاكتشاف ثغرة غير معروفة سابقًا في MONAI Label، وهو خادم مفتوح المصدر يُستخدم في أعمال التصوير الطبي. وبعد ذلك حصل المهاجمون على صلاحيات الجذر على خادم جامعي.

ما هو معلوم

تتيح الثغرة لمهاجم لا يملك حسابًا كتابة ملفات خارج المجلد الذي يحفظ فيه الخادم بياناته. وهي تؤثر في الإصدار 0.8.5 وما قبله عند تشغيله بإعداده الافتراضي. ولا يذكر المصدر رقم CVE ولا حالة التصحيح ولا تفاصيل تقنية إضافية، لذا ينبغي التأكد منها مع القائمين على المشروع.

والملفت هنا هو الأسلوب: فقد استُخدم وكلاء ذكاء اصطناعي يعملون باستقلالية لاكتشاف الضعف، لا لاستغلاله فحسب. وهذا يشير إلى أن الثغرات في الأدوات مفتوحة المصدر الأقل شهرة قد تُكتشف أسرع من السابق.

الأهمية للقطاع الصحي والبحثي

قد تشغّل المستشفيات والمراكز البحثية والجامعات في المملكة أدوات تصوير وذكاء اصطناعي خارج قوائم جرد الأنظمة السريرية المعتادة. وقد تحتوي هذه الخوادم على بيانات حساسة ويمكن الوصول إليها غالبًا من الشبكات الداخلية، لذلك يستحق اختراق بصلاحيات الجذر الانتباه حتى لو كان البرنامج مخصصًا للبحث فقط.

لا داعي للقلق المفرط، لكن مراجعة قصيرة أمر معقول: حدّدوا ما إذا كان MONAI Label مستخدمًا، وبأي إصدار، ومن يستطيع الوصول إليه.

ما يجب فعله الآن

1. ابحثوا في سجلات الأصول والبيئات البحثية عن MONAI Label وسجّلوا الإصدارات المستخدمة.
2. قيّدوا الوصول الشبكي إلى أي خادم MONAI Label بحيث لا يكون متاحًا من شبكات غير موثوقة.
3. راجعوا القنوات الرسمية للمشروع بحثًا عن إصدار مصحَّح أو إجراء تخفيف، وطبّقوه بعد التأكد منه.
4. افحصوا سجلات الخادم وكتابة الملفات بحثًا عن ملفات غير متوقعة خارج مجلد التخزين.
5. شغّلوا هذه الخدمات بأقل الصلاحيات وافصلوها عن الأنظمة التي تحوي بيانات المرضى.