وكلاء ذكاء اصطناعي يستغلون ثغرة يوم الصفر في أداة MONAI Label للتصوير الطبي، بحسب أمازون



تفيد أمازون بأن وكلاء ذكاء اصطناعي مستقلين يديرهم طرف مرتبط بالصين اكتشفوا واستغلوا ثغرة حرجة في MONAI Label. الإصدارات 0.8.5 وما قبلها متأثرة، والإصلاح مرتقب في الإصدار القادم.

- رصد فريق استخبارات التهديدات في أمازون وكلاء ذكاء اصطناعي يكتشفون ثغرة يوم صفر من نوع path traversal في MONAI Label ويستغلونها.
- انتقل الوكلاء من تحليل واجهة API إلى كتابة ملفات عشوائية على الخادم خلال نحو 11 دقيقة، ثم حصلوا لاحقاً على صلاحيات root.
- تصنّف نشرة MONAI Label الثغرة بأنها حرجة، وتشمل الإصدارات 0.8.5 وما قبلها، مع تعطيل المصادقة افتراضياً.
- تم إعداد إصلاح وسيصدر ضمن الإصدار القادم.
- تنسب أمازون النشاط بثقة متوسطة إلى جهة صينية المنشأ غير محددة، وكانت الأهداف

المرصودة جامعات في شرق آسيا.

أفادت فرق استخبارات التهديدات في أمازون بأن وكلاء ذكاء اصطناعي مستقلين، يشغّلهم طرف تهديد مرتبط بالصين، اكتشفوا واستغلوا ثغرة غير معروفة سابقاً في MONAI Label، وهي أداة مفتوحة المصدر للمساعدة بالذكاء الاصطناعي في توصيف الصور الطبية.

ما الذي حدث

رصدت أمازون النشاط في سبتمبر بعد العثور على نسخة مكشوفة من Cairn، وهو إطار مفتوح المصدر لاختبار الاختراق بالذكاء الاصطناعي. لم تكن النسخة تتطلب مصادقة، فأمكن الاطلاع على أوامر المشغّل ومخرجات الوكلاء. وأظهرت السجلات حملة استمرت نحو 48 ساعة ضد عناوين IP تعود لجامعات في شرق آسيا خارج البر الصيني.

زُوّد الوكلاء بقائمة أهداف وطُلب منهم الحصول على صلاحية shell، فحدّدوا البرنامج على أحد الأهداف، ورسموا خريطة واجهة API الخاصة به، ثم وجدوا ثغرة path traversal في وظيفة رفع الملفات. وتقول أمازون إن الانتقال من تحليل API إلى كتابة ملفات عشوائية استغرق نحو 11 دقيقة. وفي جلسة لاحقة زرع الوكلاء reverse shell بلغة Python في ملف يُنفَّذ عند كل تشغيل للمفسّر، وبلغوا صلاحيات root. ثم أُعطوا وكيلًا (proxy) يمرّ عبر نفق إلى جامعة ثانية، وترجّح أمازون أنها اخترقت بالثغرة نفسها.

استجابة المطوّرين والإسناد

نشر مطوّرو MONAI Label هذا الأسبوع نشرة تصنّف الثغرة حرجة، وتشمل الإصدارات 0.8.5 وما قبلها. المصادقة معطّلة افتراضياً، ما يتيح لأي جهة تصل إلى الخادم عبر الشبكة استغلالها. وقد أُعدّ إصلاح سيُضمَّن في الإصدار القادم. وترى أمازون بثقة عالية أنها ثغرة يوم صفر لعدم وجود إصلاح أو نشرة أو إشارة سابقة إليها. وتنسب النشاط بثقة متوسطة إلى جهة صينية المنشأ غير محددة، استناداً إلى لغة الأوامر والمنطقة الزمنية في السكربتات والأهمية الاستراتيجية المحتملة للأهداف.

الأهمية

قد تكون الجهات الصحية والبحثية التي تستخدم أدوات تصوير مفتوحة المصدر بإعداداتها الافتراضية معرّضة للخطر. وتبيّن الحادثة كيف يختصر الذكاء الاصطناعي الزمن بين الاستطلاع والاختراق.

ما يجب فعله الآن

1. حصر أي نسخ من MONAI Label، بما فيها بيئات البحث والتجارب، وتحديد الإصدارات 0.8.5 أو الأقدم.
2. تفعيل المصادقة وتقييد الوصول الشبكي إلى هذه الخوادم إلى حين توفر الإصدار المصحَّح.
3. تطبيق الإصدار المصحَّح فور نشره من مشروع MONAI Label.
4. فحص الخوادم بحثاً عن كتابة ملفات غير متوقعة أو تعديل ملفات بدء تشغيل Python أو اتصالات صادرة وأنفاق غير معتادة.
5. إدراج سيناريوهات الاختراق السريع المدفوع بالذكاء الاصطناعي في خطط الرصد والاستجابة للحوادث للأنظمة الطبية والبحثية.