أمازون: مهاجمون استخدموا إطار Cairn للذكاء الاصطناعي لاكتشاف ثغرة يوم الصفر على الأرجح في جامعات آسيوية



تفيد أمازون بأن إطار Cairn المفتوح المصدر للاختبار الآلي بالذكاء الاصطناعي ساعد مهاجمين على اكتشاف ثغرة يوم صفر على الأرجح واستغلالها في جامعات بشرق آسيا.

- رصدت أمازون في 10 سبتمبر خادم Cairn مكشوفًا تُظهر سجلاته تعليمات بالصينية المبسطة وتوقيتًا بحسب توقيت الصين.
- اكتفى المشغّل بعناوين IP وهدف محدد، وخطّط الوكلاء الآليون وعدّلوا هجماتهم دون أن يختار كل خطوة.
- فشلت معظم المحاولات، ومنها محاولة استغلال Log4Shell وتجربة أكثر من 30 ألف توليفة اعتماد على 80 اسم مستخدم.
- النجاح الوحيد كان عبر ثغرة اجتياز مسار في تطبيق ذكاء اصطناعي مفتوح المصدر للتصوير الطبي،

قيّمتها أمازون بثقة عالية على أنها يوم صفر، وقد أُصلحت لاحقًا.

- شددت أمازون على سرعة الوكلاء: عملوا 16 ساعة متواصلة وقد يتجاوزون سرعة الفرز اليدوي للتنبيهات.

أفادت فرق استخبارات التهديدات في أمازون بأن مهاجمين استخدموا Cairn، وهو إطار مفتوح المصدر للاختبار الاختراقي الذاتي بالذكاء الاصطناعي، ضد عدة جامعات في شرق آسيا. بدأ التحقيق في 10 سبتمبر عندما عثرت أمازون على خادم Cairn متاح للعامة تُظهر سجلاته تعليمات المشغّل ونشاطه.

ما الذي حدث

زوّد المشغّل الإطار بعناوين IP وطلب منه الحصول على وصول shell. ووفق CJ Moses، مسؤول أمن المعلومات في Amazon Integrated Security، خطّط الوكلاء الآليون ونفّذوا وكيّفوا أسلوبهم دون أن يوجّه المشغّل كل خطوة. وفشلت محاولات عدة، منها تشغيل من 148 إجراءً استمر 16 ساعة وشمل محاولة استغلال Log4Shell، وجهد دام ست ساعات جرّب أكثر من 30 ألف توليفة اعتماد مرتبطة بـ80 اسم مستخدم حقيقيًا.

أما المسار الناجح فكان ثغرة اجتياز مسار في تطبيق ذكاء اصطناعي مفتوح المصدر للتصوير الطبي. وتقدّر أمازون بثقة عالية أنها ثغرة يوم صفر لعدم وجود إصلاح أو نشرة أمنية أو ذكر سابق لها. وأعاد المهاجم استخدامها ضد جامعة ثانية. تواصلت أمازون مع القائمين على التطبيق فأصلحوا الخلل، وعملت AWS مع جهة حكومية لإبلاغ الجهات المتأثرة، دون الكشف عن أسماء الجامعات.

لماذا يهم ذلك

اللافت هو وتيرة التنفيذ. حذّر Moses من أن الوكيل قد يكتشف الثغرة ويستغلها أسرع مما تستطيع كثير من مراكز العمليات الأمنية فرز التنبيه يدويًا، وأن الوكلاء عملوا باستمرار دون انقطاع. وتصف تقارير حديثة أدوات هجومية مماثلة تعتمد الذكاء الاصطناعي، ويشير باحث في Gambit Security إلى أن Cairn أداة عامة الغرض، ما يجعل سلوكها أقل قابلية للتنبؤ.

لا يشير المصدر إلى أي أثر في المملكة العربية السعودية، ولم يحدد التطبيق المتأثر ولا الضحايا.

ما يجب فعله الآن

1. حصر التطبيقات المفتوحة المصدر في بيئتكم، ومنها أدوات التصوير الطبي والذكاء الاصطناعي، والتأكد من وجود مالك محدد وقناة تحديثات مراقبة لكل منها.
2. التأكد من معالجة Log4Shell في الأنظمة المكشوفة للإنترنت، وتطبيق ضوابط حماية الاعتماد مثل المصادقة متعددة العوامل والقفل ضد التخمين الكثيف لكلمات المرور.
3. مراجعة آليات الكشف والفرز لمعالجة التنبيهات عالية الخطورة على الأنظمة المكشوفة خلال دقائق، مع احتواء آلي حيث يلزم.
4. إضافة سيناريوهات هجوم مستمر تقوده وكلاء ذكاء اصطناعي إلى اختبارات الاختراق وتمارين الاستجابة للحوادث.
5. إعداد آلية لتقييم الثغرات غير المصححة في البرمجيات الخارجية ومعالجتها بإجراءات تعويضية مثل العزل

والمراقبة الإضافية.