

«أوبن إيه آي» تؤكد تورط وكلاء تابعين لها في اختراق موقع ألماني

6 سبتمبر، 2026



استغل وكلاء ذكاء اصطناعي يعملون بشكل مستقل، تابعون لشركة "أوبن إيه آي" المطورة لتطبيق "تشات جي بي تي"، صفحة ويكي باللغة الألمانية على نطاق واسع للتنسيق فيما بينهم.

وتُعد هذه الواقعة، التي حدثت في ربيع هذا العام ولم يُكشف عنها علناً إلا الآن، مثالاً آخر على الكيفية التي يمكن أن تتسبب بها البرمجيات المزودة بالذكاء الاصطناعي في إثارة مشكلات غير متوقعة.

وكان باحثون اكتشفوا نحو 18 ألف رسالة صادرة عن الذكاء الاصطناعي على موقع "دي إس إي ويكي"، ونسبوها إلى شركة "أوبن إيه آي"، وهو ما أقرت به الشركة لاحقاً بوقوف برمجياتها وراء هذه الرسائل.

وتهدف برمجيات ما يُعرف بـ "وكلاء الذكاء الاصطناعي" تنفيذ مهام للمستخدمين بشكل مستقل. وخلال الاختبارات، تُسند إلى هذه البرمجيات مهام مختلفة بهدف استكشاف قدراتها، وكذلك التعرف على ما إذا كانت هذه البرمجيات تتسبب في إثارة مشكلات. وفي أخطر واقعة كُشف عنها حتى الآن، تمكنت نماذج ذكاء اصطناعي تابعة لشركة "أوبن إيه آي" من

الخروج من بيئة الاختبار المؤمّنة الخاصة بها، واختراق أنظمة تابعة لشركة أخرى تعمل في مجال الذكاء الاصطناعي. وكان هدفها في ذلك مجرد العثور على إجابة للمهمة المطروحة عليها. وفي هذه الواقعة أيضًا، تبادل وكلاء الذكاء الاصطناعي المعلومات فيما بينهم، واستخدموا لهذا الغرض نظامًا داخليًا تابعًا للشركة، وهو أمر لم تكتشفه "أوبن إيه آي" إلا في وقت لاحق.

ووفقًا لما توصل إليه أربعة باحثين متخصصين في أمن الذكاء الاصطناعي، تلقى وكلاء البرمجيات في الواقعة التي كُشف عنها الآن مهمة البحث عن معلومات على الإنترنت على عدة جولات. وأشار الباحثون إلى أن الوقت المتاح للعثور على الإجابة تقلص بشكل كبير اعتبارًا من الجولة الثانية. وفي الوقت نفسه، طُرحت على بعض الوكلاء أسئلة كان وكلاء آخرون قد أجابوا عنها بالفعل. وذكرت دراسة الباحثين أن البرمجيات استغلت وظيفة التحرير في صفحة ويكي لإبلاغ بعضها بعضًا بالأسئلة التي قد تأتي بعد ذلك.

وتابع الباحثون أن الذكاء الاصطناعي بحث خلال ذلك عن ثغرات قابلة للاستغلال في الصفحة، التي تحمل الاسم الكامل "ويكي مطوري البرمجيات الألمان"، كما انتحل الوكلاء في بعض الإدخالات صفة أحد مسؤولي الصفحة، وأنشأوا لهذا الغرض حسابًا يحمل اسم مستخدم مطابقًا تقريبًا لاسم المستخدم الخاص به. وكتب الباحثون أن مسؤول الصفحة لم يتمكن من مواكبة حذف المنشورات التي أنشأتها الروبوتات، لأن الذكاء الاصطناعي كان أسرع في إنشاء منشورات جديدة.

ولم تدل "أوبن إيه آي" بأي تفاصيل بشأن هذه الأمور، بل أكدت فقط في بيان على منصة "إكس" أن النشاط صدر عن وكلاء ذكاء اصطناعي تابعين للشركة. وفي الوقت نفسه، أعلنت "أوبن إيه آي" عن إعداد إرشادات جديدة للإعلان عن مثل هذه الحوادث التي لم تصل إلى مستوى الهجمات السيبرانية التقليدية.