ثغرة خطيرة في «شات جي بي تي» تثير مخاوف أمنية.. بيانات المستخدمين في مرمى هجمات التصيد والاختراق

الجمعة 5 يونيو 2026 01:30 م

كشـفت تقارير أمنيـة حديثـة عن ثغرة جديـدة في أنظمـة الـذكاء الاصـطناعي التوليـدي، وعلى رأسـها «شات جي بي تي»، تتيح للمهاجمين اسـتغلال آليـة تلخيص صـفحات الإنترنت لتنفيـذ هجمات تصـيد احتيالي متطورة وجمع معلومات حساسـة عن المسـتخدمين، الأمر الذي أثار مخاوف متزايدة بشأن أمن البيانات والخصوصية في عصر الاعتماد المتسارع على أدوات الذكاء الاصطناعي.

وبحسب ما أورده موقع «ذا هاكر نيوز» المتخصـص في الأمن السـيبراني، فقد تمكن باحثون أمنيون من اكتشاف ثغرة تعتمد على ما يُعرف بـ«حقن الأوامر الخبيثة» داخل صفحات الويب، مستفيدة من قدرة نماذج الذكاء الاصطناعي على قراءة ملفات «مارك داون» (Markdown) والتعامل معها باعتبارها محتوى موثوقاً.

كيف بدأت القصة؟

يرى الباحثون أن المشـكلة تنبع من الثقة المسـبقة التي تمنحها أنظمة الذكاء الاصطناعي لبعض أنواع الملفات، وعلى رأسها ملفات «مارك داون» التي تستخدم على نطاق واسع في مواقع الإنترنت ومنصات التوثيق الرقمية.

وتتميز هـذه الملفات بإمكانيـة تضـمين روابط وصور ونصوص وأوامر مخفية داخلها، وهو ما يسـمح للمهاجمين بإدراج تعليمات خبيثة لا يراها المستخدم العادي، بينما يمكن أن تتفاعل معها نماذج الذكاء الاصطناعي أثناء تحليل أو تلخيص محتوى الصفحات.

وعنـد مطالبـة المسـتخدم للنموذج بتلخيص صـفحة ويب تحتوي على هـذه التعليمات المخفية، قد يقوم النظام بعرض محتوى ضار أو روابط احتيالية دون التمييز بينها وبين المحتوى الأصلي للصفحة.

«تصيد شات جي بي تي».. هجوم جديد بواجهة ذكية

وأطلق البـاحثون في شـركة «بريرزمو سـيكيوريتي» الأمنيـة على هـذا النوع من الهجمـات اسم «تصـيد شـات جي بي تي»، في إشارة إلى استغلال ثقة المستخدمين بالمخرجات التي يقدمها الذكاء الاصطناعي.

ويكمن الخطر في أن المسـتخدم قـد يتعامـل مع الروابط أو الصور أو التعليمات التي يعرضـها النموذج باعتبارها جزءاً من المحتوى الأصـلي الموثوق، بينما تكون في الواقع أدوات صممت خصيصاً لخداعه وسرقة بياناته أو دفعه إلى مواقع إلكترونية ضارة.

لماذا تفشل النماذج في اكتشاف الهجوم؟

ووفقا لتقرير نشره موقع «ذا ريجستر» البريطاني، فإن جذور المشكلة ترتبط بعدم قدرة نماذج الذكاء الاصطناعي الحالية على الفصل الكامل بين المحتوى الأصلي الذي تتعامل معه وبين التعليمات الخبيثة التي يتم حقنها داخل الصفحات.

وبسبب هذه المحدودية التقنية، قد تقوم الأنظمة بعرض أو تنفيذ أجزاء من المحتوى المحقون أثناء عملية التلخيص أو التحليل، ما يمنح المهاجمين نافذة جديدة للوصول إلى المستخدمين بطرق يصعب اكتشافها بالوسائل التقليدية.

وفي الوقت نفسه، لم تصدر شركة «أوبن إيه آي» أي تعليق رسمي مفصل حول هذه الثغرة أو الخطوات المحتملة لمعالجتها، بحسب ما نقلته التقارير التقنية.

ما البيانات التي يمكن أن تتعرض للخطر؟

يحذر الخبراء من أن الهجوم لا يقتصر على عرض روابط خبيثة فقط، بل قد يمتد إلى محاولة جمع معلومات تقنية عن الضحية، مثل عنوان بروتوكول الإنترنت (IP)، وبعض البيانات المتعلقة بالجهاز المستخدم أو البيئة الرقمية المحيطة به.

كما يمكن للمهاجمين تضمين أوامر تهدف إلى إرسال المعلومات التي يتم جمعها بصورة سرية إلى خوادم خارجية، بما يسمح باستخدامها لاحقاً في تنفيذ هجمات أكثر تعقيداً أو إعداد حملات تصيد موجهة بدقة أكبر.

تهديد يتجاوز «شات جي بي تي»

ويرى الباحث الأمني أندي أحمدي أن هذه المشكلة لا ترتبط بمنصة واحدة فقط، بل قد تشمل عدداً كبيراً من تطبيقات الذكاء الاصطناعي التوليدي التي تعتمد على آليات متشابهة في معالجة البيانات وتحليل المحتوى.

وأوضح أن تطور نماذج الذكاء الاصطناعي خلال السنوات الأخيرة جعلها أقرب إلى أنظمة تشغيل ومتصفحات متكاملة، وهو ما يعني أن اكتشاف الثغرات الأمنية فيها سيصبح أكثر شيوعاً مع اتساع استخداماتها وانتشارها في مختلف القطاعات.

وأضاف أن التحدي الأساسي يتمثل في أن هجمات حقن الأوامر تستغل طبيعة عمل النماذج نفسها، وليس مجرد أخطاء برمجية تقليدية يمكن إصلاحها بسهولة عبر تحديثات أمنية محدودة.

الخطر المزدوج.. من سرقة البيانات إلى اختراق الأجهزة

ويحذر الخبراء من أن خطورة هذه الهجمات لا تتوقف عند حدود تسريب المعلومات، بل تمتد إلى مرحلة أكثر تعقيداً تتمثل في دفع المستخدمين إلى التفاعل مع روابط أو أكواد استجابة سريعة (QR Codes) ضارة.

وفي حال قيام الضحية بالنقر على هذه الروابط أو مسح الأكواد باستخدام هاتفه الذكي، قد يتم توجيهه إلى مواقع مصممة لسرقة بيانات تسجيل الدخول أو تحميل برمجيات خبيثة تمنح المهاجمين صلاحيات واسعة داخل الجهاز.

وتُعد هذه المرحلة بمثابة البوابة الأولى لسلسلة من الهجمات اللاحقة التي قد تشمل الاستيلاء على الحسابات الشخصية أو الوصول إلى البيانات المخزنة أو مراقبة النشاط الرقمي للمستخدم.

تحديات أمنية جديدة في عصر الذكاء الاصطناعي

تعكس هذه الثغرة جانباً من التحديات الأمنية المتزايدة التي تواجه قطاع الذكاء الاصطناعي، في ظل توسع الاعتماد على هذه الأدوات في العمل والتعليم والبحث والتواصل اليومي.

ومع استمرار تطور قدرات النماذج الذكية، يؤكد خبراء الأمن السيبراني أن حماية المستخدمين لن تعتمد فقط على تحديثات الشركات المطورة، بل ستتطلب أيضاً رفع مستوى الوعي الرقمي وتوخي الحذر عند التعامل مع الروابط والمحتوى الذي يتم توليده أو عرضه عبر أنظمة الذكاء الاصطناعي.

ويجمع المختصون على أن هجمات حقن الأوامر تمثل واحدة من أخطر التحديات المستقبلية أمام شركات الذكاء الاصطناعي، نظراً لارتباطها المباشر بالبنية التشغيلية للنماذج نفسها، وهو ما يجعل مواجهتها أكثر تعقيداً من الثغرات البرمجية التقليدية.

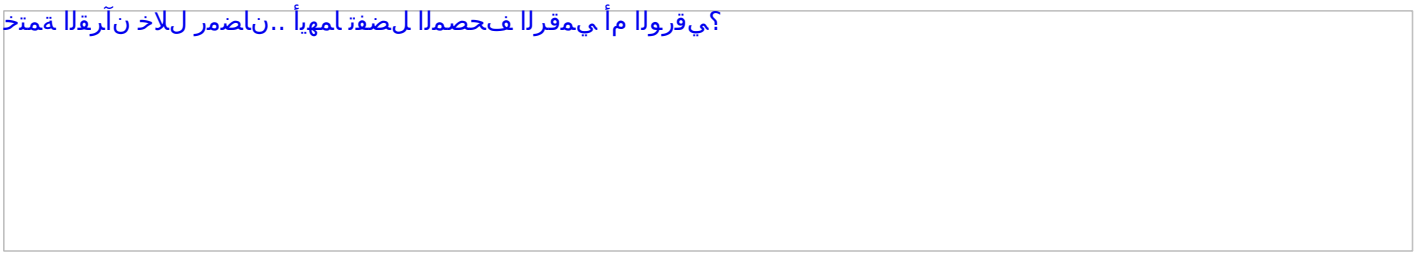
اقتصاد

الـ"شعبة" تعترف: ارتفاع أسعار الأسماك والفسيخ والرنجة 30% بسبب الوقود
الثلاثاء 14 أبريل 2026 09:00 م

اقتصاد

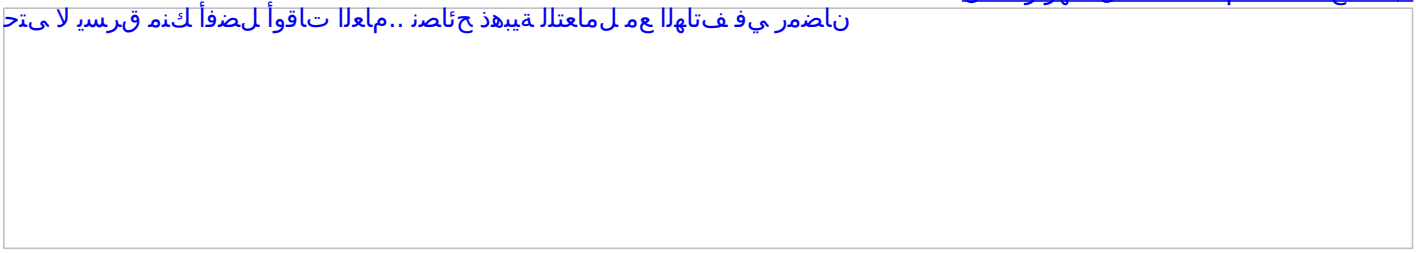
بالصور: إصابة 18 طالبة في حادث أتوبيس بطريق الصعيد الحر بالمنيا
الخميس 9 أبريل 2026 11:20 م

مقالات متعلقة



ختمة القرآن خلال رمضان.. أيهما تفضل المصحف الرقمي أم الورقي؟

4 نصائح لاستخدام هاتفك خلال شهر رمضان



حتى لا يسرق منك أفضل أوقات العام.. نصائح ذهبية للتعامل مع الهاتف في رمضان

كيف تتخلص من السموم الرقمية خلال شهر رمضان؟

كيف تتخلص من السموم الرقمية خلال شهر رمضان؟