جوجل تسرّع تحديثات كروم لمواجهة ثغرات الذكاء الاصطناعي

الجمعة 11 سبتمبر 2026 10:30 م

لم تعد سرعة اكتشاف الثغرات الأمنية في متصفحات الإنترنت تسمح بانتظار أسابيع طويلة قبل إصدار الإصلاحات، خصوصا مع تطور أدوات الذكاء الاصطناعي وقدرتها المتزايدة على تحليل الشيفرات البرمجية ورصد نقاط الضعف التي قد يستغلها المهاجمون.
وفي هذا السياق، بدأت شركة جوجل في إعادة صياغة آلية التعامل مع أمن متصفح كروم، عبر تقليص الفترة الزمنية بين التحديثات الأمنية، والاستعانة بشكل أكبر بنماذج الذكاء الاصطناعي في البحث عن الثغرات.

وأعلنت جوجل تسريع وتيرة إطلاق تحديثات كروم الأمنية، بحيث تصدر التحديثات مرة كل أسبوعين بدلا من مرة كل أربعة أسابيع في السابق.
وتأتي الخطوة في إطار استراتيجية أمنية جديدة تستهدف التعامل بصورة أسرع مع الثغرات المكتشفة، سواء من خلال أنظمة الشركة وأدوات الذكاء الاصطناعي أو عبر الباحثين والمستخدمين الذين يبلغون عن المشكلات الأمنية.

ويرتبط هذا التغيير بالتطور السريع في طبيعة التهديدات الإلكترونية، بعدما أصبح الذكاء الاصطناعي عاملا مؤثرا في جانبي المواجهة، إذ يمكن استخدامه في اكتشاف نقاط الضعف وتحليل البرمجيات، وفي الوقت نفسه يمكن أن يساعد المهاجمين على تطوير هجمات إلكترونية أكثر تعقيدا وسرعة.

تحديثات أمنية بوتيرة أسرع

أوضحت جوجل، في بيان مصاحب لإطلاق النسخة رقم 153 من متصفح كروم، أن تغيير جدول التحديثات يأتي ضمن توجه أمني يستهدف مواكبة المرحلة الجديدة التي فرضها انتشار تقنيات الذكاء الاصطناعي.

ويشمل المتصفح أنظمة الحواسيب المكتبية، إلى جانب الهواتف العاملة بنظامي أندرويد وآيفون، ما يجعل أي ثغرة أمنية فيه ذات نطاق واسع بالنظر إلى العدد الكبير من المستخدمين والأجهزة التي تعتمد عليه يوميا.

وتراهن الشركة على تقليص المدة بين التحديثات في الحد من الفترة التي يمكن خلالها استغلال الثغرات بعد اكتشافها، إذ إن سرعة إصدار الإصلاح الأمني تمثل عاملا مهما في حماية المستخدمين، خاصة عندما تكون الثغرة معروفة أو قابلة للاستغلال قبل وصول التصحيح إلى جميع الأجهزة.

ولا يقتصر اكتشاف الثغرات على فرق الأمن التابعة لجوجل، إذ تستقبل الشركة أيضا بلاغات من مجتمع الباحثين والمستخدمين.
ومع زيادة عدد الثغرات التي يمكن اكتشافها باستخدام أدوات آلية، يصبح التعامل معها خلال فترة أقصر أمرا أكثر أهمية.

الذكاء الاصطناعي يدخل قلب الحماية

يعتمد جزء متزايد من جهود جوجل الأمنية على نماذج الذكاء الاصطناعي والوكلاء القادرين على تحليل كميات ضخمة من الشيفرات البرمجية والبحث عن أنماط قد تشير إلى وجود خلل أمني.

ووفقا لتقارير تقنية، استخدمت جوجل وكلاء للذكاء الاصطناعي في عمليات البحث عن الثغرات داخل كروم، وتمكنت هذه الأدوات من المساعدة في العثور على أكثر من ألف ثغرة أمنية، بلغ عددها 1072 ثغرة وفقا لما أورده موقع سايبر سيكيورتي نيوز.

وتعكس هذه الأرقام تحولا في الطريقة التي تتعامل بها شركات التكنولوجيا مع أمن البرمجيات، فبدلا من الاعتماد بصورة أساسية على المراجعة البشرية، أصبحت تقنيات الذكاء الاصطناعي قادرة على فحص مساحات واسعة من الشيفرات خلال وقت أقصر، مع إمكانية إعادة تحليل أجزاء سبق فحصها بحثا عن نقاط ضعف لم تكن واضحة في المراجعات السابقة.

ولا يعني ذلك الاستغناء عن فرق الأمن السيبراني، وإنما يضيف إلى أدواتها وسيلة جديدة يمكنها تسريع عمليات البحث والتحقق، قبل أن تتحول الثغرات إلى وسيلة فعلية لاختراق الأجهزة أو الوصول إلى البيانات.

ثغرة ظلت مخفية 13 عاما

من أبرز الأمثلة على أهمية هذا النهج، اكتشاف فريق الأمن السيبراني في كروم ثغرة ظلت موجودة لأكثر من 13 عاما دون أن يتم رصدها.

وجرى اكتشاف الثغرة من خلال وكلاء للذكاء الاصطناعي طورتهم جوجل اعتمادا على نموذج جيميناي، حيث عملت الأدوات على تحليل أجزاء من الشيفرات المرتبطة بمتصفح كروم والمكونات الموجودة في مشروع كروميوم مفتوح المصدر.

وتكتسب الثغرة أهمية خاصة بسبب موقعها داخل البيئة الاختبارية للمتصفح. فالبيئة المعزولة أو ما يعرف بالصندوق الاختباري يفترض أن تمنع الشيفرات التي تعمل داخله من الوصول إلى أجزاء أخرى حساسة من المتصفح أو نظام التشغيل.

لكن الثغرة المكتشفة كانت تتيح للشيفرات تجاوز هذا العزل، وهو ما قد يسمح لها بالوصول إلى بيانات داخل المتصفح أو إلى ملفات موجودة على الحاسوب في ظروف معينة.

ويكشف العثور على ثغرة بهذا العمر أن بعض نقاط الضعف يمكن أن تظل بعيدة عن الانتباه لسنوات طويلة، حتى مع عمليات التدقيق الأمني المستمرة. كما يوضح الدور الذي يمكن أن تؤديه أدوات الذكاء الاصطناعي في إعادة فحص البرمجيات القديمة من زوايا مختلفة.

كيف تبحث جوجل عن الثغرات

لا تعتمد وكلاء الذكاء الاصطناعي الذين تستخدمهم جوجل على طريقة واحدة في تحليل شيفرات كروم، وإنما يمكنهم الاستفادة من مجموعة واسعة من المصادر والبيانات المرتبطة بآلية عمل المتصفح.

وتشمل عملية البحث مراجعة الشيفرات المصدرية، والنظر في الثغرات التي سبق اكتشافها، والاستفادة من مستندات الأمن السيبراني، إلى جانب تحليل طريقة عمل المتصفح وذاكرته والمكونات المختلفة التي يعتمد عليها.

وتسمح هذه المنهجية للأنظمة الذكية ببناء صورة أوسع عن الطريقة التي يمكن أن يتصرف بها أحد مكونات المتصفح في ظروف غير متوقعة، وهو ما قد يساعد في الكشف عن مشكلات لا تظهر عند اختبار الوظائف الأساسية بصورة منفصلة.

كما أن قدرة الذكاء الاصطناعي على تحليل كميات كبيرة من المعلومات قد تمنح فرق الأمن إمكانية إجراء عمليات بحث متكررة بوتيرة أعلى، بدلا من الاكتفاء بمراجعات دورية تعتمد بالكامل على الوقت المتاح للباحثين.

سباق جديد بين المتصفحات

يأتي تسريع التحديثات الأمنية في وقت يشهد فيه سوق متصفحات الإنترنت منافسة متزايدة، بالتزامن مع محاولة شركات التكنولوجيا إدخال الذكاء الاصطناعي بصورة مباشرة في تجربة التصفح.

ولم يعد المتصفح مجرد أداة لفتح المواقع والبحث عبر الإنترنت، إذ تتجه شركات عدة إلى تطوير متصفحات قادرة على فهم طلبات المستخدم، وتنفيذ مهام متعددة، وتحليل محتوى الصفحات، والاستفادة من أدوات الذكاء الاصطناعي أثناء التصفح.

وتواجه جوجل في هذا المجال منافسة من متصفحات متعددة، من بينها فايرفوكس وبرايف، إلى جانب متصفحات أحدث تحاول تقديم تجربة تصفح قائمة على الذكاء الاصطناعي، مثل ديا وكوميت، فضلا عن متصفح داك داك جو الذي يركز بدرجة أكبر على الخصوصية.

ومع تحول الذكاء الاصطناعي إلى عنصر رئيسي في المنافسة بين المتصفحات، تصبح الحماية الأمنية جزءا أساسيا من قدرة أي متصفح على الحفاظ على المستخدمين، خصوصا أن إضافة مزايا ذكية جديدة قد تفتح في الوقت نفسه مساحات جديدة تحتاج إلى تأمين ومراجعة مستمرة.