

رصد محاولة استغلال لثغرات PHP2Shell قبل الإفصاح العلني عنها بأربعة أيام



رصد فريق استخبارات التهديدات في أمازون محاولة لاستغلال ثغرات PHP2Shell في 17 أكتوبر 2026 قبل الإفصاح العلني عنها، ثم تحدثت التقارير عن استغلال واسع بعد صدور الإصلاحات.

- رصد فريق استخبارات التهديدات في أمازون المحاولة في 17 أكتوبر 2026 ضد خدمة MadPot الخادعة.
- وقعت المحاولة قبل الإفصاح العلني عن الثغرات بنحو أربعة أيام.
- صدرت المحاولة من عنوان IP مرتبط بشبكة تجارية لإخفاء الهوية.
- تتعرض الثغرات حاليًا لاستغلال واسع في الواقع بعد صدور الإصلاحات.

أفاد فريق استخبارات التهديدات في أمازون برصد محاولة لاستغلال ثغرات PHP2Shell المعلن عنها حديثًا، وذلك في 17 أكتوبر 2026. استهدف النشاط خدمة MadPot الخادعة، ووقع قبل نشر تفاصيل الثغرات بنحو أربعة أيام.

ما الذي جرى رصده

بحسب التقرير، صدرت المحاولة من عنوان IP مرتبط بشبكة تجارية لإخفاء الهوية. ولا يقدم المصدر تفاصيل إضافية عن الجهة التي تقف خلفها أو عن الطبيعة التقنية للثغرات.

ويذكر التقرير أيضًا أن الثغرات تتعرض الآن لاستغلال واسع في الواقع بعد صدور الإصلاحات. وهذا النمط، الذي يتحرك فيه المهاجمون قبل الإفصاح أو بعده مباشرة، يقلص الوقت المتاح للمؤسسات للاستجابة.

الدلالة للمؤسسات

تشير المحاولة المبكرة إلى أن انتظار الإفصاح العلني قد لا يكون افتراضًا آمنًا للأنظمة المكشوفة على الإنترنت. وعلى المؤسسات التي تشغل تطبيقات مبنية على PHP أن تعدّ ذلك دافعًا للتحقق من تعرضها وحالة التحديثات دون تأخير.

ولأن المصدر لا يذكر الإصدارات المتأثرة ولا معرّفات الإصلاحات، ينبغي للفرق الرجوع إلى نشرات المورّد أو المشروع للتفاصيل. وفي الأثناء، قد تساعد مراجعة السجلات للفترة التي سبقت الإفصاح وما حولها على كشف أي استطلاع مبكر.

والأولوية العملية واضحة: تحديد مواضع استخدام PHP، وتطبيق الإصلاحات المتاحة عبر إجراءات التغيير الطارئ، ومراقبة مؤشرات الاستغلال.

ما يجب فعله الآن

1. حصر التطبيقات والخوادم المكشوفة على الإنترنت التي تستخدم PHP، بما فيها التي يديرها أطراف ثالثة أو تُستضاف خارجيًا.
2. تطبيق إصلاحات PHP2Shell عبر إجراء التغيير الطارئ، مع الرجوع إلى نشرات المورّد لمعرفة الإصدارات المتأثرة.
3. مراجعة سجلات الويب والتطبيقات منذ ما قبل 17 أكتوبر 2026 بحثًا عن طلبات غير معتادة أو مؤشرات اختراق.
4. رفع مستوى المراقبة على أحمال PHP المكشوفة، والنظر في ضوابط مؤقتة عبر جدار حماية تطبيقات الويب حيث يتأخر التحديث.
5. مطالبة مزوّد الخدمات المُدارة والاستضافة بتأكيد حالة التحديث كتابيًا.