تأكيد استغلال ثغرات PHP2Shell فعلياً: حدّثوا PHP وراجعوا التعرّض



تأكد استغلال ثغرتَي تنفيذ الأوامر عن بُعد الحرجتين في PHP المعروفتين باسم PHP2Shell استغلالًا ناجحاً، وفق رصد عبر مصائد خداعية. التحديثات متاحة منذ 21 أكتوبر.

- الثغرتان CVE-2026-109618 وCVE-2026-109619 حرجتان لتنفيذ الأوامر عن بُعد وتُعرفان معاً باسم PHP2Shell.
- سجّلت مصيدة خداعية تنفيذاً مؤكداً للأوامر ضد Apache mod_php يعمل بإصدار PHP 8.4.26.
- أوضح الباحث أن البيئة كانت مواتية بعامل واحد، ولا يعكس ذلك موثوقية الاستغلال في بيئات أخرى.
- أصدر فريق أمن PHP التحديثات في 21 أكتوبر.
- توجد ثغرة RCE منفصلة بلا تصحيح هي CVE-2026-115560، وتخفيفها بضبط session.upload_progress.enabled=0.

ما الذي حدث

تم استغلال ثغرتين حرجتين لتنفيذ الأوامر عن بُعد في PHP، هما CVE-2026-109618 وCVE-2026-109619 وتُعرفان معاً باسم **PHP2Shell**، استغلالًا ناجحاً في العالم الفعلي. رصد ذلك الباحث Adel Karimi من Perplexity عبر مصائد خداعية سجّلت تنفيذاً مؤكداً للأوامر ضد تثبيت Apache mod_php يعمل بإصدار PHP 8.4.26، وأكد النتائج Marcus Hutchins من Expel.

وأشار Karimi إلى أن الدليل جاء من بيئة mod_php مواتية عمداً بعامل واحد، ولا يقيس موثوقية الاستغلال مع أعداد عوامل أخرى أو إصدارات PHP أو تطبيقات مختلفة.

الخلفية

أصدر فريق أمن PHP التصحيحات في 21 أكتوبر. وقد تسرّبت تفاصيل وبعض أكواد إثبات المفهوم قبل ذلك، لكن الفريق ذكر أن أياً منها لم يكن فعالًا. ورصدت شركات أمنية عدة وAmazon Threat Intelligence محاولات قبل الإفصاح، وُصفت كلها بأنها غير ناجحة إلى حين هذا التأكيد. ونشرت CISA قاعدة كشف SIGMA لمحاولات الاستغلال، ولم تكن قد أدرجت الثغرات ضمن المستغَلّة وقت كتابة المصدر.

وعلى صعيد منفصل، نشر فريق PHP إجراءً تخفيفياً لثغرة RCE أخرى هي CVE-2026-115560، لا يتوفر لها تصحيح بعد ولا تُستغل إلا بتركيبة غير معتادة من الإعدادات وشيفرة التطبيق. ويُنصح بضبط session.upload_progress.enabled=0 حتى صدور الإصلاح.

لماذا يهم ذلك

تعمل PHP على نحو 70% من المواقع، وتقدّر VirusTotal وجود أكثر من 5.1 مليون مضيف PHP مكشوف على الإنترنت. ينبغي للجهات اعتبار تطبيقات PHP المواجهة للإنترنت أولوية للتحديث والمراجعة.

ما يجب فعله الآن

1. حصر تطبيقات ومضيفات PHP المواجهة للإنترنت، بما فيها نشرات Apache mod_php، وتوثيق إصدارات PHP.
2. تطبيق تحديثات PHP الأمنية الصادرة في 21 أكتوبر عبر إدارة التغيير الطارئة، بدءاً بالأنظمة المكشوفة.
3. ضبط session.upload_progress.enabled=0 حيثما قد تنطبق CVE-2026-115560 إلى حين صدور تصحيح.
4. تطبيق قاعدة SIGMA الصادرة عن CISA في نظام SIEM ومراجعة سجلات الويب والعمليات منذ منتصف أكتوبر بحثاً عن نشاط مشبوه.
5. تصعيد أي اختراق مؤكد وفق خطة الاستجابة للحوادث، والإبلاغ للهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي بحسب الالتزامات.