PHP تصدر تحديثات طارئة لثغرتين حرجتين للتنفيذ عن بُعد ضمن مجموعة PHP2Shell



أصدر فريق أمن PHP تحديثات للثغرتين CVE-2026-109618 وCVE-2026-109619، وهما ثغرتا تنفيذ أوامر عن بُعد دون مصادقة. وقد رُصدت هجمات مبكرة، لذا يُنصح بالتحديث العاجل.

- ثغرتان للتنفيذ عن بُعد دون مصادقة، CVE-2026-109618 وCVE-2026-109619، تُتابعان معًا باسم PHP2Shell.
- تؤثران على PHP التي تخدم طلبات الويب، ومنها PHP-FPM وphp-cgi mod_php وFrankenPHP وLiteSpeed، والخطر الأعلى مع mod_php.
- الإصدارات المصححة هي PHP 8.5.12 و8.4.27 و8.3.36 و8.2.35، أما 8.1 وما قبله فلم تعد تتلقى تحديثات من المشروع.
- أفادت Cloudflare برصد هجمات مبكرة قبل صدور التحديثات.
- التدابير المؤقتة تقلل التعرض ولا تمنع الهجمات كليًا، والتحديث هو الحماية الدائمة.

أصدر فريق أمن PHP تحديثات طارئة لثغرتين حرجتين للتنفيذ عن بُعد، هما CVE-2026-109618 وCVE-2026-109619، وتُتابعان معًا باسم **PHP2Shell**. ويمكن استغلال كلتيهما دون مصادقة. وقد اكتشفهما باحثون من Calif وWiz وOpenAI.

ما الأنظمة المتأثرة

تنشأ الثغرتان من مشكلة واحدة: قد تترك PHP ذاكرتها في حالة تالفة عند انتهاء الطلب بشكل غير طبيعي. وتطال تثبيتات PHP التي تخدم طلبات الويب، ومنها PHP-FPM وApache مع mod_php وphp-cgi وFrankenPHP وLiteSpeed. ويرى فريق PHP أن الخطر الأعلى مع mod_php، إذ ثبت وجود استغلال يعمل قبل تنفيذ أي كود تطبيقي. ويتم تنفيذ الكود بصلاحيات حساب عامل الويب.

وتُستخدم PHP على نطاق واسع، ومنها أنظمة إدارة المحتوى مثل WordPress وJoomla وDrupal. وتشير تقديرات VirusTotal الواردة في المصدر إلى أكثر من 5.1 مليون مضيف PHP متاح عبر الإنترنت.

الإصلاحات والتدابير المؤقتة

على مسؤولي خوادم PHP 8.x تثبيت الإصدار 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35، وعلى مستخدمي PHP 7 أو أقدم الانتقال إلى إصدار مصحح. ولا يتلقى PHP 8.1 وما قبله تحديثات من المشروع، وإن كان بعض موزعي التوزيعات ومزودي الدعم طويل الأمد يقدمون إصلاحات مُرحَّلة، كما أصدر فريق PHP إصلاحات مبسطة من المصدر للإصدارات 7.4 و8.0 و8.1.

وأفادت Cloudflare برصد هجمات مبكرة، وبأن قواعد WAF لديها مؤقتة فقط. ونصح المركز الوطني للأمن السيبراني في المملكة المتحدة بالتحديث أو إيقاف الأنظمة المتأثرة. أما تدابير PHP المنشورة، مثل ضبط memory_limit=-1 وخفض post_max_size وتعطيل session.upload_progress، فتقلل بعض مسارات الهجوم دون حماية كاملة، ويبقى التحديث الدفاع الدائم الوحيد.

ما يجب فعله الآن

1. حصر جميع الخوادم والتطبيقات التي تعمل بـ PHP، بما فيها أنظمة إدارة المحتوى والحاويات، وتحديد الإصدارات ونمط التشغيل (mod_php وPHP-FPM وغيرها).
2. الترقية إلى PHP 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35 كتغيير طارئ، مع إعطاء الأولوية للأنظمة المكشوفة على الإنترنت وعمليات mod_php.
3. في حال PHP 8.1 أو أقدم، الحصول على إصلاح مُرحَّل من المورد أو الانتقال إلى إصدار مدعوم، والنظر في إيقاف الأنظمة المكشوفة إن تأخر التحديث.
4. عند تعذر التحديث فورًا، تطبيق تدابير PHP المنشورة وإعادة تشغيل العمال، مع اعتبارها مؤقتة فقط.
5. مراجعة سجلات الويب وجدار WAF بحثًا عن طلبات غير معتادة أو أعطال، وتصعيد أي اشتباه باختراق عبر مسار الاستجابة للحوادث.