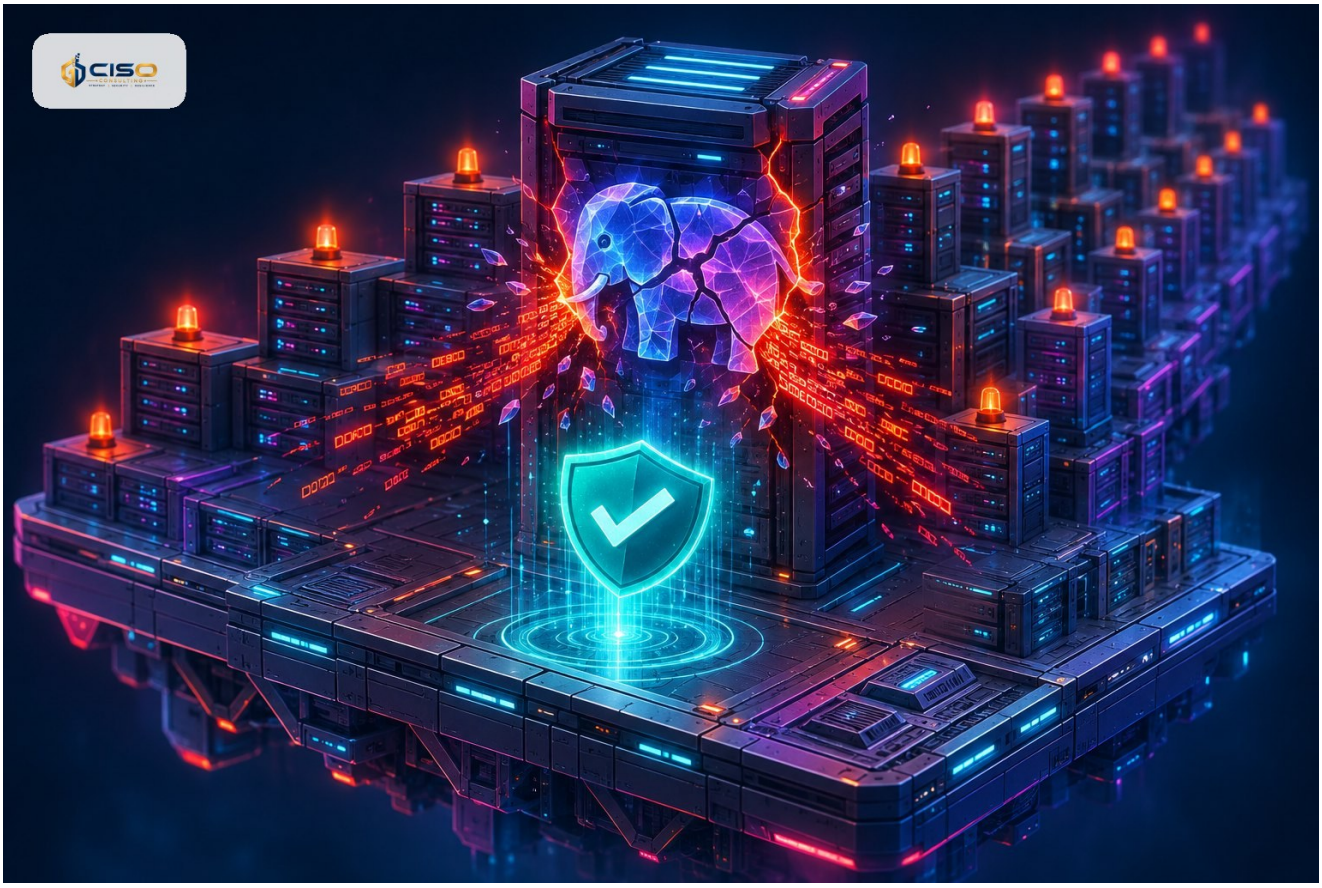
ثغرتان حرجتان في PHP قيد الاستغلال الفعلي: حدّثوا إلى الإصدارات المصححة الآن



أصدرت PHP تحديثًا طارئًا لثغرتين حرجتين تتيحان تنفيذ تعليمات برمجية عن بُعد. يجري استغلالهما فعليًا، ويتأثر بإحداهما على الأقل كل إصدار صدر خلال العقد الماضي.

- تتيح CVE-2026-109618 وCVE-2026-109619 للمهاجم تنفيذ تعليمات برمجية من اختياره على خادم مصاب.
- الإصلاحات متوفرة في PHP 8.5.12 و8.4.27 و8.3.36 و8.2.35، والخوادم المتأثرة تشغّل PHP 5.4 أو أحدث.
- أفادت Cloudflare برصد بعض محاولات الاستغلال، وفعّلت قواعد جدار حماية تطبيقات الويب عند 3:02 فجرًا بالتوقيت العالمي.
- تتوقع Wiz استغلالاً واسعًا لزرع web shells، وتشبّه حجم المشكلة بثغرة Log4Shell.
- رصدت Censys نحو 2.58 مليون مضيف متصل بالإنترنت و54.9 مليون موقع ويب يعمل بـ PHP.

أصدرت PHP تحديثًا أمنيًا طارئًا يعالج ثغرتين حرجتين تحملان الرقمين CVE-2026-109618 وCVE-2026-109619. تتيح كل منهما للمهاجم تنفيذ تعليمات برمجية من اختياره على خادم مصاب. ويفيد خبراء ورد ذكرهم في التقرير بوجود برمجيات استغلال تعمل، وبأن الاستغلال الفعلي بدأ.

النطاق المتأثر

تقوم منصات نشر كثيرة على PHP، منها Drupal وMagento وJoomla وWordPress. تؤثر الثغرتان في خوادم الويب التي تشغّل PHP 5.4 أو أحدث، وتذكر Wiz أن كل إصدار صدر خلال العقد الماضي يتأثر بواحدة منهما على الأقل. وتتوفر الإصلاحات في PHP 8.5.12 و8.4.27 و8.3.36 و8.2.35.

نقلت Reuters أن مواقع حكومية في أوروبا ودول أخرى توقفت عن العمل بعد الإفصاح. وذكرت Cloudflare أنها رصدت بعض الاستغلال وفعّلت قواعد جدار حماية تطبيقات الويب عند 3:02 فجرًا بالتوقيت العالمي. وحددت Censys نحو 2.58 مليون مضيف متصل بالإنترنت و54.9 مليون موقع ويب يعمل بـ PHP.

أهمية الأمر

تتوقع Wiz استغلالاً واسع النطاق بهدف زرع **web shells** التي تمنح المهاجمين تحكمًا عن بُعد في الموقع. وتشير إلى أن PHP متغلغلة في التطبيقات بحيث قد تواجه المؤسسات صعوبة في التحديث لفترة، وتشبّه الوضع بـ Log4Shell عام 2021. وتصدر الجهات المصنِّعة تحديثاتها؛ فقد أطلقت Ubuntu حزم PHP محدّثة، ويتابع SANS Internet Storm Center منصات أخرى.

ما زال الوضع يتطور، لذا ينبغي مراجعة نشرات الجهات المصنِّعة باستمرار. وقد تخفف قواعد جدار حماية التطبيقات من التعرض، لكنها لا تغني عن تحديث PHP نفسه.

ما يجب فعله الآن

1. حصر جميع الخوادم المتصلة بالإنترنت والداخلية التي تشغّل PHP، بما فيها الخوادم خلف منصات إدارة المحتوى مثل Drupal وMagento وJoomla وWordPress.
2. الترقية إلى PHP 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35، أو تثبيت الحزمة المصححة الصادرة عن مورّد نظام التشغيل.
3. مطالبة مزوّدي الاستضافة ووكالات الويب بتأكيد كتابي لحالة التحديث على الأنظمة التي تستضيف مواقعكم.
4. تفعيل قواعد جدار حماية تطبيقات الويب الخاصة بهاتين الثغرتين أو التحقق منها كطبقة مؤقتة ريثما يكتمل التحديث.
5. البحث عن web shells وعن ملفات أو عمليات غير متوقعة على خوادم PHP، ورفع أي اكتشاف عبر مسار الاستجابة للحوادث.
6. التخطيط لترقية أي خادم يعمل على فرع PHP منتهي الدعم، إذ لم تُذكر إصلاحات إلا للإصدارات الأربعة أعلاه.