

فريق PHP يحذّر من ثغرتين حرجتين قبيل إصدار تحديثات طارئة



يعتزم فريق أمن PHP إصدار تحديثات طارئة في 21 أكتوبر لمعالجة ثغرتين حرجتين بتقييم 9.2 وفق CVSS v4.0، بعد تسرّب معلومات عنهما، ولم تُرصد أي استغلالات فعلية.

- أعلن فريق PHP عن تحديثات أمنية في 21 أكتوبر الساعة 14:00 بالتوقيت العالمي لمعالجة ثغرتين، لكل منهما تقييم 9.2 وفق CVSS v4.0.
- قد يُقدّم موعد الإصدار إذا انتشرت التفاصيل علناً أو ظهر استغلال فعلي.
- تفيد watchTower بأن الثغرتين CVE-2026-109618 و CVE-2026-109619 تتيجان تنفيذ شيفرة عن بُعد، ويُعتقد أنهما تمسّان الإصدارات 5 و6 و7 و8.
- لم ترصد watchTower أي استغلال فعلي حتى الآن، وتقول إنها نجحت في إعادة إنتاج CVE-2026-109618.
- لم تُنشر بعدُ التفاصيل الرسمية ولا الإصدارات المتأثرة ولا الإصدارات المصحّحة.

طلب فريق أمن PHP من مسؤولي الأنظمة الاستعداد لتحديثات أمنية طارئة يوم الأربعاء 21 أكتوبر الساعة 14:00 بالتوقيت العالمي، لمعالجة ثغرتين حرجيتين تحمل كل منهما تقييم 9.2 وفق CVSS v4.0. وتقوم على PHP مواقع كثيرة وأنظمة إدارة محتوى ومنصات تجارة إلكترونية وخدمات ويب مخصصة.

ما هو معروف حتى الآن

لم يكشف الفريق بعد عن التفاصيل التقنية أو الإصدارات المتأثرة أو الإصدارات التي ستتضمن الإصلاح، وذكر أنه سينشرها عند صدور التحديثات. كما احتفظ بحق تقديم الإصدار إذا أصبحت التفاصيل علنية أو ظهر استغلال فعلي. وأفادت شركة watchTower لموقع BleepingComputer بأن الثغرتين هما CVE-2026-109618 و CVE-2026-109619، وأنهما تتيحان تنفيذ شيفرة عن بُعد، ويُعتقد أنهما تؤثران في الإصدارات 5 و6 و7 و8 من PHP. وذكرت أن معلومات عنهما تسربت قبل موعد الإفصاح المحدد، وأنها أعادت إنتاج CVE-2026-109618، ولم ترصد استغلالاً فعلياً. وتجدر الإشارة إلى أن watchTower وصفت الثغرتين بتقييم CVSS 10.0 وذكرت موعد إفصاح مختلفاً، بينما يذكر إعلان PHP الرسمي تقييم 9.2 وفق CVSS v4.0 وإصداراً في 21 أكتوبر. ويُعدّ الإعلان الرسمي المرجع، أما ما ورد عن الإصدارات المتأثرة من الباحثين فلم يتأكد بعد.

الخطوات العملية

بما أن التفاصيل لم تُنشر، فالأولوية للاستعداد: معرفة أماكن تشغيل PHP ومالك كل نظام، وسرعة اختبار التحديث ونشره فور صدوره.

ما يجب فعله الآن

1. حصر جميع الأنظمة المعرّضة للإنترنت والداخلية التي تعمل بـ PHP، بما فيها أنظمة إدارة المحتوى والتجارة الإلكترونية والتطبيقات المخصصة، مع إصداراتها ومالكها.
2. تجهيز نافذة تغيير طارئة وبيئة اختبار يوم 21 أكتوبر للتحقق من التحديث ونشره بسرعة.
3. متابعة إعلان PHP الرسمي وقائمة ANNOUNCE البريدية، فقد يصدر التحديث قبل الموعد المعلن.
4. التأكد من تغطية جدار حماية تطبيقات الويب والسجلات لتطبيقات PHP ومراقبة الطلبات أو النشاط غير المعتاد إلى حين التحديث.
5. تحديد إصدارات PHP المنتهية الدعم وتخطيط ترقيتها أو عزلها، إذ لم يتأكد بعد شمول الإصلاحات للإصدارات القديمة.