CERT-EU: ثغرات حرجة في PHP تتيح تنفيذ التعليمات عن بُعد دون مصادقة وتستدعي التحديث الفوري



أفاد CERT-EU بثغرتين حرجتين في PHP تتيحان تنفيذ التعليمات عن بُعد دون مصادقة، وقد صدرت إصلاحاتهما. أمثلة الاستغلال متداولة، وثمة ثغرة ثالثة لها إجراء تخفيف فقط.

- الثغرتان CVE-2026-109618 وCVE-2026-109619 بدرجة CVSS تبلغ 9.2 لكل منهما، وقد تتيحان تنفيذ التعليمات عن بُعد دون مصادقة.
- صدرت الإصلاحات في الإصدارات 8.5.12 و8.4.27 و8.3.36 و8.2.35، أما PHP 8.1 وما قبله فلا يتلقى تحديثات من المشروع.
- التفاصيل التقنية منشورة وأمثلة الاستغلال متداولة، ما يرجّح أن الاستغلال قد بدأ فعلًا.
- الثغرة الثالثة CVE-2026-115560 تمس فقط تطبيقات الويب ذات الإعداد غير المعتاد، ولن يصدر لها إصدار استثنائي.
- كل بيئات PHP التي تخدم طلبات الويب معرضة للخطر، وتُعد mod_php الأعلى خطورة.

ما الذي حدث

أعلن مشروع PHP في 20 أكتوبر 2026 عن إصدار أمني يعالج ثغرتين حرجتين، ونُشرت الإصلاحات في 21 أكتوبر. ويشير CERT-EU إلى أن كلتيهما قد تتيحان تنفيذ التعليمات عن بُعد دون مصادقة، وأن التفاصيل التقنية تُناقش علناً وبدأت أمثلة الاستغلال الأولية بالتداول، ما يزيد احتمال أن يكون المهاجمون قد بدأوا استغلالهما.

تتعلق **CVE-2026-109618** بتلف الذاكرة عندما يُجهض PHP طلباً تجاوز حد الذاكرة، فتبقى بيانات الطلب مهيأة جزئياً. أما **CVE-2026-109619** فتتعلق ببقاء حالة داخلية قديمة بعد تحرير ذاكرتها، ثم استخدامها في طلب لاحق ضمن العملية نفسها. وقد أثبت استغلال تجريبي أن طلباً واحداً دون مصادقة يكفي لإطلاق الهجوم قبل تنفيذ أي شيفرة تطبيق.

وفي 23 أكتوبر أعلن PHP عن ثغرة ثالثة هي CVE-2026-115560 تتيح تنفيذ التعليمات عن بُعد، لكنها تمس فقط تطبيقات الويب ذات الإعداد غير المعتاد، ويرى المشروع أن خطرها غير مرجح، ولن يصدر لها إصدار استثنائي. وستُنشر تفاصيلها الكاملة مع الإصدار القادم.

من المتأثر

أي تثبيت PHP يخدم طلبات الويب معرّض للخطر، بما في ذلك PHP-FPM وApache مع mod_php وphp-cgi وFrankenPHP وLiteSpeed. وتشمل الإصدارات المتأثرة ما يسبق 8.5.12 و8.4.27 و8.3.36 و8.2.35، إضافة إلى الإصدارات المنتهية الدعم. وقد تتأثر كذلك منتجات تجارية ومفتوحة المصدر تعتمد على PHP حتى لو لم يكن مكشوفاً مباشرة، ويوجّه CERT-EU إلى مستودع NCSC-NL لتحديد هذه البرمجيات.

الاستجابة الموصى بها

يُوصى بالتحديث فوراً إلى إصدار مُصلَح، أو الحصول على حزم مُحدّثة من مزود التوزيعة أو الدعم طويل الأمد. وإن تعذّر التحديث فيمكن النظر في عزل التطبيقات المكشوفة للإنترنت عن الشبكات العامة حتى تطبيق الإصلاح والتحقق منه. أما إجراءات التخفيف المؤقتة فتقلل التعرض لمسارات هجوم محددة ولا تجعل التثبيت آمناً. وبالنسبة إلى CVE-2026-115560، يُنصح بتعطيل session.upload_progress.enabled وإعادة تشغيل جميع العمليات حتى الإصدار الدوري القادم.

ما يجب فعله الآن

1. حصر جميع تطبيقات PHP المكشوفة للإنترنت مع إصدارات PHP وأنماط التشغيل (mod_php و-PHP FPM وغيرها).
2. الترقية إلى 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35، أو الحصول على حزم مُحدّثة من مزود التوزيعة أو الدعم طويل الأمد، ثم التحقق من النتيجة.
3. التخطيط للترحيل أو لإصلاحات مُعادة الإسناد من المزود للإصدار PHP 8.1 وما قبله لأنه لا يتلقى تحديثات من المشروع.
4. الاستفسار من موردي المنتجات الخارجية عمّا إذا كانت تتضمن PHP، مع الاستعانة بمستودع NCSC-NL مرجعاً.
5. عند تعذر التحديث الفوري، عزل التطبيقات المكشوفة عن الشبكات العامة وتطبيق إجراءات التخفيف الموثقة مع اعتبارها حلًا جزئياً.

6. ضبط session.upload_progress.enabled=0 على مستوى الخادم وإعادة تشغيل جميع العمليات، ومراجعة سجلات الويب وجدار حماية التطبيقات بحثاً عن طلبات غير مصادَق عليها مشبوهة.