

PHP تُصدر تحديثًا طارئًا لمعالجة ثغرتين حرجتين للتنفيذ عن بُعد



تنشر PHP إصدارًا طارئًا في 21 أكتوبر الساعة 14:00 بالتوقيت العالمي لمعالجة ثغرتين حرجتين بدرجة 9.2 وفق CVSS v4.0. وتفيد watchTower بأنهما تتيحان التنفيذ عن بُعد، ولم يُبلغ عن استغلال.

- صنف فريق أمن PHP ثغرتين حرجتين بدرجة 9.2 وفق CVSS v4.0.
- يصدر الإصدار ضمن إصدار طارئ خارج الدورة المعتادة في 21 أكتوبر الساعة 14:00 بالتوقيت العالمي.
- يفيد باحثو watchTower بأن الثغرتين تتيحان تنفيذ التعليمات البرمجية عن بُعد.
- الفروع من 8.2 إلى 8.5 فقط هي التي ستتلقى الإصلاح.
- لم يُبلغ عن أي استغلال حتى الآن، ولم تُنشر تفاصيل الثغرتين.

ما الذي أُعلن

ستنشر جهة تطوير PHP تحديثاً أمنياً طارئاً خارج دورة الإصدارات المعتادة في 21 أكتوبر الساعة 14:00 بالتوقيت العالمي، لمعالجة ثغرتين صنّفهما فريقها الأمني بدرجة 9.2 وفق مقياس CVSS v4.0. ولم يصف الفريق الثغرتين علناً.

ويقول باحثو watchTower، الذين أطلقوا على المسألة اسم PHP2Shell، إن الثغرتين تتيحان **تنفيذ التعليمات البرمجية عن بُعد**. ولم يُبلّغ عن أي استغلال حتى الآن.

من سيتلقى الإصلاح

الفروع الأربعة المدعومة فقط، من PHP 8.2 إلى 8.5، يمكنها تلقي الإصلاح. أما الأنظمة العاملة على فروع أقدم فلا يشملها هذا الإصدار بحسب المصدر، ولذلك تحتاج إلى خطة معالجة مستقلة.

ما يعنيه ذلك للمنشآت

نظراً لقلّة التفاصيل المتاحة، تكمن الأولوية العملية في الجاهزية لا في ردّ الفعل. فعند صدور التحديث ينبغي أن تكون الفرق التي تشغّل PHP في تطبيقات الويب والبوابات والأدوات الداخلية قادرة على تحديد الأنظمة المتأثرة وتحديثها بسرعة. وقد تُنشر التفاصيل التقنية بعد الإصدار، فتقصر المدة بين النشر ومحاولات الاستغلال المحتملة، وإن كان المصدر لا يذكر أي نشاط من هذا النوع.

وينبغي للمنشآت أن تمنح تطبيقات PHP المكشوفة على الإنترنت أولوية أولى، وأن تتأكد من أن الإصدارات التي تشغّلها ضمن الفروع المدعومة.

ما يجب فعله الآن

1. حصر جميع الأنظمة والتطبيقات التي تعمل بـ PHP، بما فيها التطبيقات الخارجية والمستضافة، وتسجيل إصدارات الفروع.
2. تحديد تطبيقات PHP المكشوفة على الإنترنت ومنحها أولوية التحديث فور صدور الإصدار.
3. التخطيط لنافذة تغيير طارئة في 21 أكتوبر لاختبار التحديث ونشره دون تأخير.
4. رصد أي أنظمة تعمل بفروع أقدم من 8.2 وتحديد قرار الترقية أو الضوابط التعويضية.
5. رفع مستوى مراقبة سجلات خوادم الويب والتطبيقات للكشف عن أي سلوك غير معتاد على خوادم PHP.