

ثغرات حرجية في PHP تتيح تنفيذ أوامر عن بُعد دون مصادقة: حدّثوا الآن



يبحث المركز الوطني للأمن السيبراني البريطاني على التحرك الفوري لمعالجة ثغرتين حرجيتين في PHP هما CVE-2026-109618 و CVE-2026-109619، قد تتيحان تنفيذ أوامر عن بُعد دون مصادقة. وقد أصدرت PHP تحديثاً.

- ثغرتان حرجتان في PHP هما CVE-2026-109618 و CVE-2026-109619 قد تسمحان للمهاجم بتنفيذ أوامر على أي خادم ويب يشغل PHP.
- قد يؤدي استنفاد الذاكرة إلى تلف في الذاكرة، ويمكن استغلاله في ظروف معينة لتنفيذ تعليمات برمجية عن بُعد دون مصادقة.
- الإصدارات من PHP 5 فصاعداً متأثرة، وعلى مستخدمي الإصدارات الأقدم الانتقال إلى إصدار مدعوم بالكامل.
- قد تتأثر أيضاً المنتجات والأجهزة التي تضمّن PHP ضمن مكوناتها.

- تتوفر إجراءات تخفيف مؤقتة، وإن تعذر تطبيقها يوصي المركز بالنظر في إيقاف النظام عن الشبكة.

دعا المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC) المؤسسات إلى التحرك الفوري لمعالجة مشكلة أمنية حرجية في PHP، وهي لغة برمجة تعمل من جهة الخادم وتستخدم على نطاق واسع لتوليد محتوى الصفحات الديناميكي والتعامل مع قواعد البيانات وتشغيل منطق التطبيقات الخلفي. كما أن PHP مضقنة في عدد من المنتجات الأخرى.

طبيعة الثغرتين

يمكن للمهاجم افتعال حالة استنفاد للذاكرة (OOM) في PHP تؤدي إلى تلف في الذاكرة، ويمكن استغلال ذلك في ظروف معينة لتنفيذ تعليمات برمجية عن بُعد دون مصادقة. وقد عالجت PHP المشكلة. والمعرّفان هما:

- **CVE-2026-109618**: تنفيذ تعليمات عن بُعد عبر استنفاد الذاكرة أثناء تحليل المدخلات وفق RFC 1867.
- **CVE-2026-109619**: تنفيذ تعليمات عن بُعد عبر تلف الحالة العامة بعد خطأ جسيم.

تشمل الثغرتان المؤسسات التي تستخدم PHP من الإصدار 5 فصاعداً، ويحث مستخدمو الإصدارات الأقدم على الانتقال إلى إصدار مدعوم بالكامل. ويذكر المركز أنه سيواصل رصد الأثر على المؤسسات البريطانية.

الاستجابة الموصى بها

ينصح المركز بحصر جميع منصات PHP بدءاً بالأنظمة المكشوفة على الإنترنت، وعدم الاقتصار على الإصدارات القديمة. كما يوصي بالتحديث إلى أحدث إصدار مصحّح، وتطبيق خطوات التحصين الصادرة عن فريق PHP، ومتابعة تحديثات الموردين للأجهزة والخدمات التي تضمّن PHP. وقد نشر NCSC-NL قائمة بالمنتجات ذات الاعتماد على PHP التي قد تتأثر.

إذا تعذر التحديث فقد وفّر فريق PHP إجراءات تخفيف مؤقتة. وإن لم يكن تطبيقها سريعاً ممكناً، يقترح المركز النظر في إيقاف النظام عن الشبكة. أما الأنظمة التي يتعذر تحديثها أو تعطيلها فوراً فينبغي فحصها بحثاً عن مؤشرات اختراق وأبواب خلفية قبل الترقية أو التخفيف.

ما يجب فعله الآن

1. حصر جميع منصات PHP بدءاً بالأنظمة المكشوفة على الإنترنت بغض النظر عن الإصدار.
2. تحديث PHP إلى أحدث إصدار مصحّح وتطبيق خطوات التحصين الصادرة عن فريق PHP.
3. مطالبة موردي الأجهزة والتطبيقات التي تضمّن PHP بإصدارات مصحّحة، ومراجعة قائمة NCSC-NL للمنتجات المتأثرة.
4. عند تأخر التحديث، تطبيق إجراءات التخفيف المؤقتة من فريق PHP، أو إيقاف النظام عن الشبكة إن تعذر ذلك.
5. فحص الأنظمة غير المحدّثة بحثاً عن مؤشرات اختراق وأبواب خلفية، مع الاستعانة بدعم الاستجابة للحوادث عند الحاجة.

6. نقل الأنظمة العاملة بإصدارات PHP غير المدعومة إلى إصدار مدعوم وتوثيق ذلك ضمن إدارة الثغرات.