

CISA تحثّ على التحديث الفوري لثغرتين حرجتين في PHP: CVE-2026-109618 و CVE-2026-109619



تحثّ CISA على التحديث الفوري لثغرتين حرجتين في PHP تُعرفان باسم "php2shell" وتتيحان تنفيذ الأوامر عن بُعد دون مصادقة. لم يُرصد استغلال وقت النشر، لكن الأنظمة غير المحدّثة معرّضة للخطر.

- الثغرتان CVE-2026-109618 و CVE-2026-109619 المعروفتان باسم "php2shell" تتيحان تنفيذ الأوامر عن بُعد دون مصادقة.
- تتأثر جميع شبيّات PHP التي تعالج طلبات الويب.
- الإصدارات المصحّحة هي PHP 8.5.12 و 8.4.27 و 8.3.36 و 8.2.35.
- لم ترصد CISA أي استغلال وقت النشر.
- الإصداران 8.1 وما قبله غير مدعومين، ويوصى بإيقاف الأنظمة التي يتعذر تحديثها.

دعت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) المؤسسات إلى معالجة ثغرتين حرجيتين في PHP دون تأخير، هما CVE-2026-109618 و CVE-2026-109619. وتُعرفان معًا باسم "php2shell"، وتتيحان لمهاجم غير مصادق تنفيذ تعليمات برمجية عن بُعد. وتشمل جميع تثبيتات PHP التي تعالج طلبات الويب.

ما المتأثر وما الحل

توجد المعالجة في الإصدارات PHP 8.5.12 و 8.4.27 و 8.3.36 و 8.2.35. وتذكر CISA أنها لم ترصد استغلالاً لهاتين الثغرتين عند نشر التنبيه، إلا أن الأنظمة غير المحدّثة تبقى معرضة للخطر. أما الإصدار 8.1 وما قبله فغير مدعوم. وتنبّه CISA أيضًا إلى أن PHP كثيرًا ما يكون مضمّنًا في برمجيات أخرى، فقد لا يظهر وجوده في سجل الأصول المعتاد.

الاستجابة الموصى بها

يرتكز توجيه CISA على تحديد مواقع PHP ثم تحديثه ومراقبة أي إساءة استخدام:

- حصر جميع الأنظمة التي تشغّل أي إصدار من PHP، بما فيها الأنظمة التي يأتي فيها مكوّنًا مضمّنًا.
- التحديث الفوري بدءًا بالأنظمة المكشوفة على الإنترنت.
- إيقاف الأنظمة المعتمدة على PHP إن تعذّر تحديثها سريعًا أو كانت تعمل بالإصدار 8.1 أو أقدم.
- استخدام جدار حماية تطبيقات الويب حمايةً مؤقتة فقط، وليس بديلًا عن التحديث.
- رصد قيام عمليات PHP بتشغيل أوامر شل أو تنزيل أدوات.

كما ينبغي للفرق مراجعة نشرة PHP الأمنية الرسمية لمعرفة تفاصيل المعالجة. وبالنسبة للجهات الخاضعة للتنظيم، تبقى الأولوية لحصر شامل للأصول، إذ إن المكوّنات المخفية هي الثغرة الأرجح.

ما يجب فعله الآن

1. حصر جميع الأنظمة التي تشغّل PHP، بما فيها المنتجات التي تضمّنه.
2. الترقية إلى PHP 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35 بدءًا بالأنظمة المكشوفة على الإنترنت.
3. إيقاف الأنظمة المعتمدة على PHP إن تعذّر تحديثها سريعًا أو كانت تعمل بالإصدار 8.1 أو أقدم.
4. تفعيل قواعد جدار حماية تطبيقات الويب أو تشديدها كإجراء مؤقت.
5. تنبيه فريق المراقبة الأمنية إلى عمليات PHP التي تشغّل أوامر شل أو تنزّل أدوات.
6. توثيق التعرّض والمعالجة ضمن إجراءات إدارة الثغرات والتغيير.