

CISA تحث على التحديث الفوري لثغرتين حرجتين في PHP تُعرفان باسم php2shell



تحث CISA على التحديث الفوري لثغرتي CVE-2026-109618 و CVE-2026-109619 في PHP اللتين تتيحان تنفيذ تعليمات عن بُعد دون مصادقة. لم يُرصد استغلال حتى الآن، والإصدارات المصححة متاحة.

- ثغرتان حرجتان في PHP هما CVE-2026-109618 و CVE-2026-109619 تُعرفان معًا باسم php2shell.
- تتيح الثغرتان تنفيذ تعليمات عن بُعد دون مصادقة، وتؤثران في كل تثبيتات PHP التي تخدم طلبات الويب.
- الإصدارات المصححة هي PHP 8.5.12 و 8.4.27 و 8.3.36 و 8.2.35.
- لم ترصد CISA استغلالاً للثغرتين وقت النشر.
- إصدارات PHP 8.1 وما قبلها لم تعد تتلقى تحديثات، ويُنصح بعزل الأنظمة المتأثرة عن الإنترنت.

دعت CISA المؤسسات بقوة إلى معالجة ثغرتين حرجيتين في PHP هما CVE-2026-109618 و CVE-2026-109619، وتُعرفان معًا باسم "php2shell".

ما الذي تأثر

تتيح الثغرتان لمهاجم دون مصادقة تنفيذ تعليمات عن بُعد، وتشملان كل تثبيت لـ PHP يخدم طلبات الويب. والإصدارات المصححة هي PHP 8.5.12 و 8.4.27 و 8.3.36 و 8.2.35. وتشير CISA إلى أنها لم ترصد استغلالاً وقت نشر التنبيه، لكن الأنظمة غير المحدثة تبقى معرضة للخطر.

توصيات CISA

تنصح CISA بحصر جميع الأنظمة التي تعمل بأي إصدار من PHP أولاً. وتكمن أهمية ذلك في أن PHP كثيرًا ما يكون مكوّنًا داخل برمجيات أخرى، فقد لا يكون وجوده واضحًا. ثم تُطبّق التحديثات فور توفرها مع إعطاء الأولوية للأنظمة المكشوفة على الإنترنت.

وإذا تعذر التحديث الفوري، أو كانت الأنظمة تعمل بإصدار PHP 8.1 أو أقدم، وهي إصدارات لم تعد تتلقّى تحديثات، فتوصي CISA بعزل هذه الأنظمة عن الإنترنت إلى حين ترقيتها. وقد يوفر جدار حماية تطبيقات الويب حماية مؤقتة، لكنه لا يغني عن التحديث.

الأهمية للجهات المنظمة

قد يكون التعرض كاملاً في منتجات أطراف ثالثة، لذا فإن الحصر هو الخطوة الأكثر عرضة للنقص. وينبغي للمؤسسات سؤال مورديها عما إذا كانت منتجاتهم تتضمن PHP، ومتابعة المعالجة عبر إجراءات إدارة الثغرات والتغيير المعتمدة.

ما يجب فعله الآن

1. حصر جميع الأنظمة ومنتجات الأطراف الثالثة التي تشغّل PHP أو تتضمنه، بما فيها ما لا يظهر وجوده مباشرة.
2. التحديث إلى PHP 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35 بدءًا بالأنظمة المكشوفة على الإنترنت.
3. عزل الأنظمة التي يتعذر تحديثها سريعًا أو التي تعمل بـ PHP 8.1 أو أقدم عن الإنترنت حتى يتم تحديثها.
4. استخدام جدار حماية تطبيقات الويب كإجراء مؤقت فقط وليس بديلاً عن التحديث.
5. مطالبة الموردين بتأكيد تضمّن منتجاتهم لـ PHP وموعد توفير الإصلاحات.