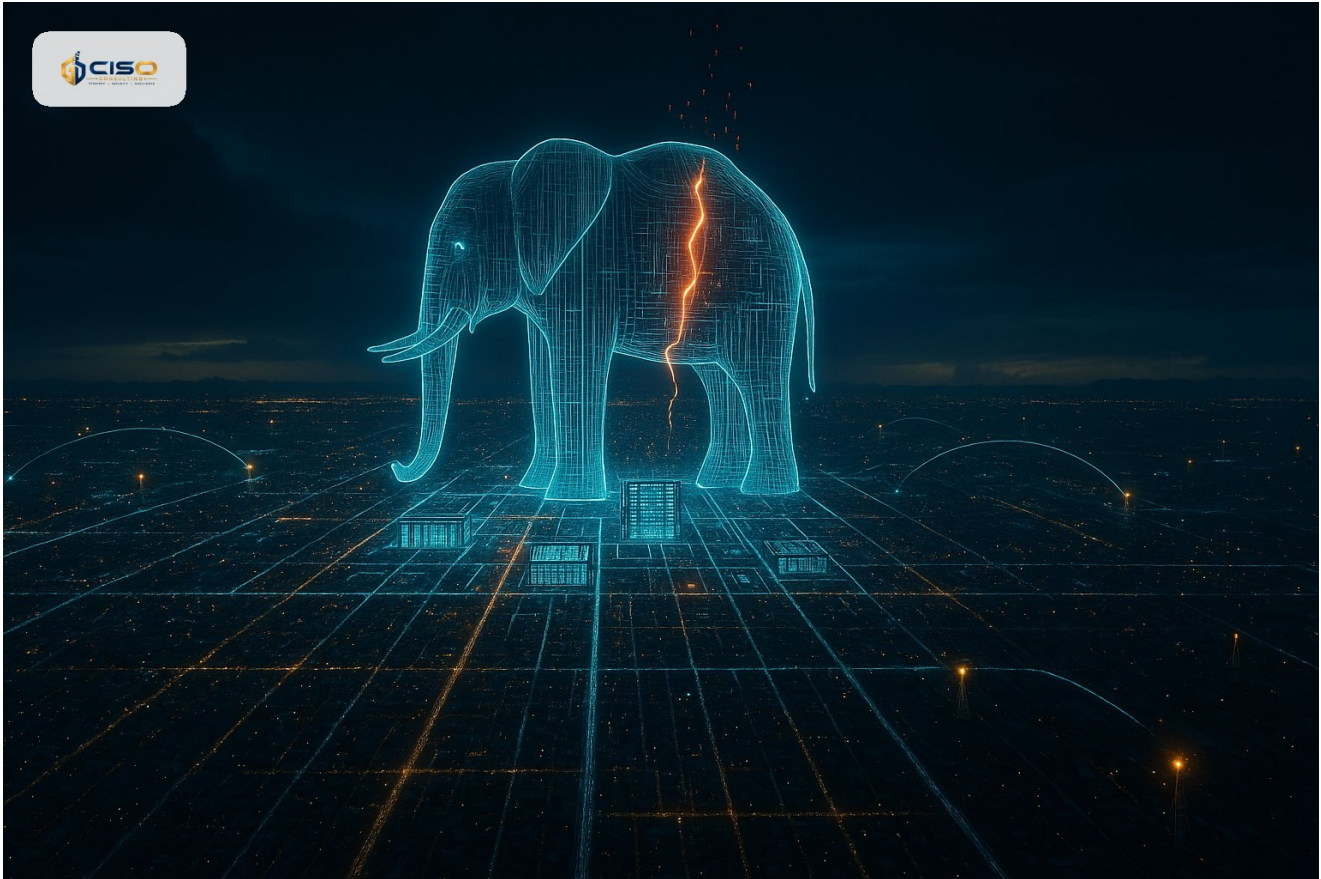


ثغرتان حرجتان في PHP (CVE-2026-109618 و CVE-2026-109619): الاستعداد لتحديث الإصدار



أعلن PHP.net عن تحديث حرج، ورفع SANS ISC مستوى InfoCon إلى الأصفر بسبب انتشار PHP الواسع وتقدير الخطورة بـ 9.4 على CVSS وتوفر استغلالات تجريبية قبل صدور التصحيح.

- أعلن PHP.net عن تحديث حرج يصدر في اليوم نفسه الذي نُشرت فيه مدونة SANS ISC.
- الثغرتان مسجلتان برقمي CVE-2026-109618 و CVE-2026-109619.
- الخطورة المتوقعة 9.4 على مقياس CVSS.
- تتوفر استغلالات تجريبية مبكرة قبل صدور التصحيح.
- رفع SANS ISC مستوى InfoCon إلى الأصفر بسبب الانتشار الواسع لـ PHP.

ما الذي أُعلن

أعلن PHP.net أنه سينشر تحديثاً حرجياً. وردّ مركز SANS Internet Storm Center، الذي يتابع مستوى التهديدات على الإنترنت، برفع مستوى InfoCon إلى الأصفر. وتحمل الثغرتان الرقمين CVE-2026-109618 و CVE-2026-109619.

أهمية الأمر

ذكر SANS ISC ثلاثة أسباب لهذا القرار: الانتشار الواسع لـ PHP، والخطورة المتوقعة البالغة 9.4 على مقياس CVSS، وتوفر استغلالات تجريبية مبكرة قبل صدور التصحيح. وهذا الأمر الأخير يقلّص الفترة بين الإعلان وإمكانية وقوع الهجمات. ولا يوضح المصدر الطبيعة التقنية للثغرتين ولا الإصدارات المتأثرة ولا وجود استغلال فعلي، لذا ينبغي التحقق من هذه التفاصيل في ملاحظات الإصدار الرسمية لـ PHP عند نشرها.

الخطوات المقترحة

على الجهات التي تشغّل مواقع أو بوابات أو تطبيقات داخلية مبنية على PHP أن تستفيد من الوقت السابق لصدور التصحيح في تحديد أماكن استخدام PHP والجهة المسؤولة عن كل نظام ومدى سرعة اختبار التحديث وتطبيقه. وتأتي الأنظمة المكشوفة على الإنترنت في المقدمة. تابعوا الإعلان الرسمي لـ PHP وطبقوا التحديث عبر إدارة التغيير المعتمدة مع مسار طارئ للإصلاحات الحرجة.

ما يجب فعله الآن

1. حصر جميع الأنظمة والتطبيقات التي تعمل بـ PHP وبدء ذلك بالمكشوفة على الإنترنت.
2. تحديد مسؤول عن كل نظام PHP واعتماد نافذة زمنية للاختبار والتطبيق.
3. متابعة إعلان PHP.net الرسمي وملاحظات الإصدار لمعرفة الإصدارات المتأثرة والمصححة.
4. تطبيق التحديث عبر مسار التغيير الطارئ فور توفره واختباره.
5. تكثيف مراقبة سجلات خوادم الويب والتطبيقات على أنظمة PHP إلى حين التصحيح.