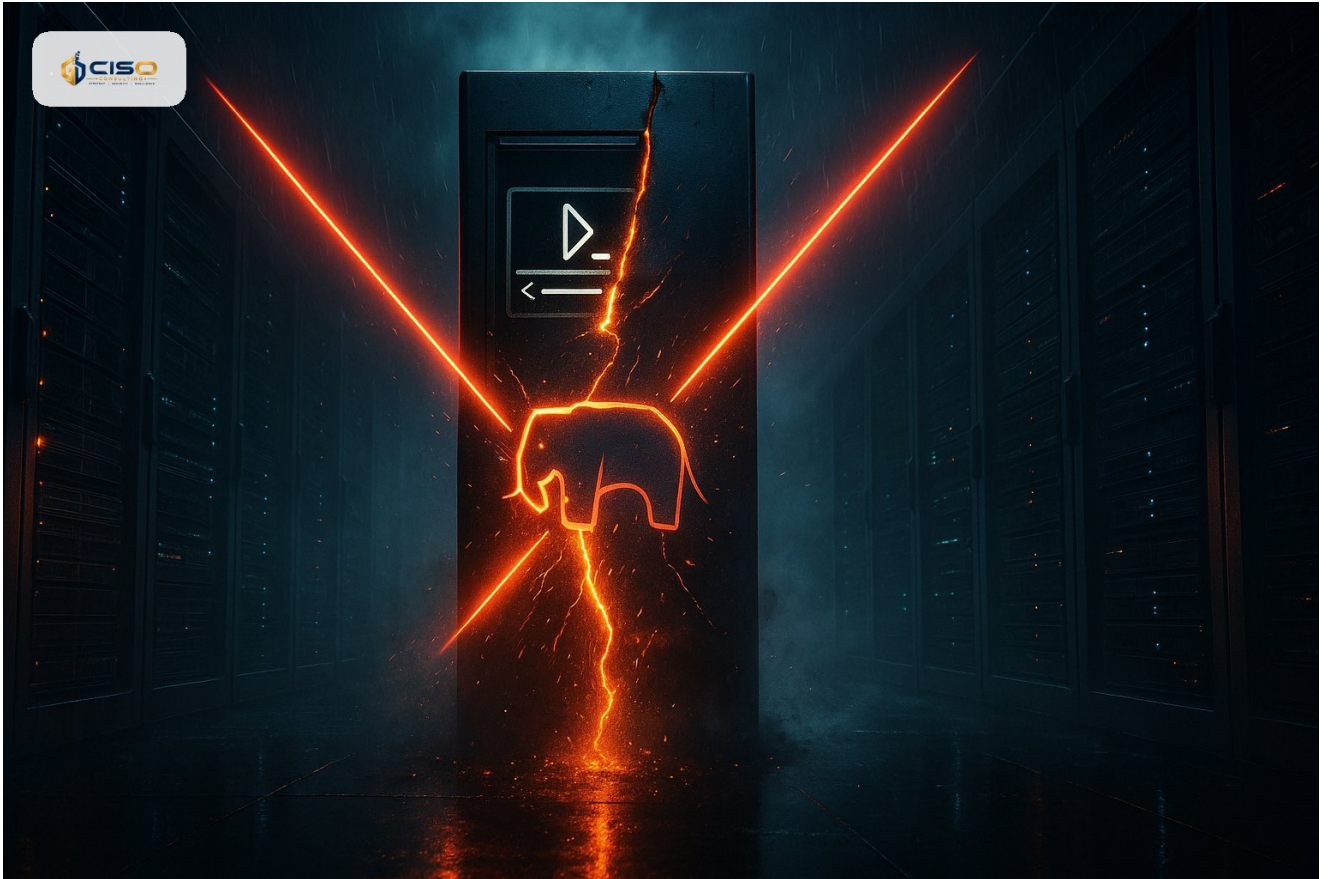


PHP تصدر تحديثات طارئة لثغرتين حرجتين للتنفيذ عن بُعد ضمن PHP2Shell



أصدرت PHP تحديثات طارئة لثغرتين حرجتين في بيئة التشغيل تُعرفان معاً باسم PHP2Shell، تتيحان لمهاجم دون حساب تنفيذ تعليمات برمجية على الخادم. وقد ظهرت محاولات استغلال، ولا يحمي الخادم بالكامل إلا التحديث.

- ثغرتان حرجتان تُعرفان معاً باسم PHP2Shell تتيحان لمهاجم دون حساب تنفيذ تعليمات برمجية على خادم الويب.
- الثغرتان في بيئة تشغيل PHP نفسها لا في أي تطبيق، لذا يتعرض الموقع للخطر حتى لو كانت شيفرته سليمة.
- الإصدارات المصححة هي PHP 8.5.12 و8.4.27 و8.3.36 و8.2.35.
- يؤكد فريق PHP أن التحديث وحده يحمي الخادم حماية كاملة.
- ظهرت محاولات استغلال للثغرتين.

أصدرت PHP تحديثات أمنية طارئة لمعالجة ثغرتين حرجيتين في اللغة نفسها. تُعرف الثغرتان معاً باسم PHP2Shell، وتتيحان لمهاجم لا يملك حساباً تنفيذ تعليمات برمجية على خادم الويب.

ما الذي يتأثر

تقع الثغرتان في بيئة تشغيل PHP وليس في تطبيق بعينه. ويعني ذلك أن الموقع قد يكون معرضاً للخطر حتى لو كانت شيفرته مكتوبة ومُدارة بإحكام. وتتضمن الإصدارات PHP 8.5.12 و8.4.27 و8.3.36 و8.2.35 الإصلاحات اللازمة. ويشير فريق PHP إلى أن التحديث هو الإجراء الوحيد الذي يحمي الخادم حماية كاملة.

وقد ظهرت بالفعل محاولات استغلال، لذا فإن تأخر تحديث الأنظمة خطر عملي وليس نظرياً فقط.

الخطوات المقترحة

ينبغي على الجهات التي تشغل مواقع أو بوابات أو أدوات داخلية مبنية على PHP أن تحدد أولاً أماكن استخدامه، بما في ذلك الاستضافة لدى أطراف ثالثة والتطبيقات التي يديرها الموردون. ثم تنقل كل نظام إلى الإصدار المصحح المناسب لفرعه الحالي وتتأكد من تطبيق التحديث فعلياً.

لا يذكر المصدر حلاً مؤقتة ولا الشروط التقنية للاستغلال، لذا يُنصح بالرجوع إلى ملاحظات الإصدار الرسمية من PHP. وإذا تعذر التحديث قبل نافذة التغيير، فيُعامل النظام على أنه عالي الخطورة مع تكثيف مراقبة خوادم الويب المعنية.

ما يجب فعله الآن

1. حصر جميع الأنظمة التي تعمل بـ PHP، بما فيها التطبيقات المستضافة لدى أطراف ثالثة أو التي يديرها الموردون.
2. الترقية إلى PHP 8.5.12 أو 8.4.27 أو 8.3.36 أو 8.2.35 بحسب الفرع المستخدم، ثم التحقق من الإصدار بعد التحديث.
3. إعطاء الأولوية لخوادم الويب المواجهة للإنترنت عند اعتماد التغيير الطارئ.
4. تكثيف مراقبة سجلات خوادم الويب وسلوكها بحثاً عن مؤشرات محاولات الاستغلال إلى حين اكتمال التحديث.
5. مطالبة الموردين ومزودي الاستضافة بتأكيد كتابي بأن بيئات PHP لديهم قد جرى تحديثها.