PHP تُصلح ثغرة phpAfterShell الحرجة في معالجة الجلسات المرتبطة بـ PHP2Shell



أصلحت PHP الثغرة CVE-2026-126714 (درجة CVSS: 9.2) في كتابة ملفات الجلسات، وقد تتيح تنفيذ التعليمات عن بُعد وفق شروط محددة. ولم تُسجَّل حالات استغلال فعلي.

- الثغرة CVE-2026-126714 المسماة phpAfterShell درجتها 9.2 وفق CVSS، وأُصلحت في 19 نوفمبر مع ست مشكلات حرجة أخرى.
- تكتب PHP فوق ملف الجلسة دون تفريغه أولًا، فإذا انقطعت العملية بقي مزيج من بيانات جديدة وقديمة قد يُفضي إلى إلغاء تسلسل كائنات.
- يتطلب الاستغلال شروطاً عدة، منها التخزين الافتراضي للجلسات ومسار استغلال مثل تتبع تقدم الرفع ومسار من إلغاء التسلسل إلى تنفيذ التعليمات.
- الإصدارات المصححة هي PHP 8.6.0 و8.5.13 و8.4.28 و8.3.37 و8.2.36.
- لم تُسجَّل حالات استغلال فعلي حتى الآن.

أصلحت PHP ثغرة حرجة تحمل الرمز CVE-2026-126714، وأطلقت عليها شركة Depthfirst اسم phpAfterShell. درجتها 9.2 وفق CVSS، وقد عولجت في 19 نوفمبر مع ست مشكلات حرجة أخرى.

طبيعة الثغرة

تكتب PHP فوق ملف الجلسة من بدايته دون تفريغه أولًا. فإذا انقطعت الكتابة قبل خطوة البتر اللاحقة، يبقى في الملف بيانات جلسة جديدة تليها بقايا الجلسة القديمة. وتفيد Depthfirst بوجود طرق موثوقة لمقاطعة العملية أثناء تحديثات تقدم رفع الملفات في الجلسة، ما يتيح لمهاجم دمج جزء من جلسة صحيحة مع جزء من أخرى. وعندما تعالج عملية لاحقة هذه البيانات التالفة على أنها حالة مشروعة، يتحكم المهاجم في قيم الجلسة ويستطيع تشغيل إلغاء تسلسل الكائنات، وهو ما قد يفضي إلى **تنفيذ تعليمات عن بُعد**.

وترتبط الثغرة بـ PHP2Shell، وهي ثغرة سابقة كانت دالة رد النداء الخاصة بتقدم الرفع تفك ترميز جلسة مخزنة في ملف قبل بدء السكربت المستهدف. وقد قيّدت PHP الكائنات التي يمكن إنشاؤها، لكنها لم تغيّر سلوك تحديث الملف الأساسي.

الشروط والوضع الحالي

الاستغلال ليس يسيراً؛ إذ يتطلب تخزين الجلسات الافتراضي، ومسار استغلال (أسهلها تتبع تقدم الرفع)، وتوقف عملية PHP أثناء الكتابة، وطلباً يستدعي session_start() على الملف التالف، ومساراً من إلغاء التسلسل إلى تنفيذ التعليمات. وتشير نشرة PHP إلى أن المشكلة قد تنشأ أيضاً حين يخزن تطبيق نصوصاً كبيرة يتحكم بها المستخدم داخل الجلسة، وأن إخفاقاً في حد الذاكرة في خيط آخر ضمن الإصدارات متعددة الخيوط قد ينهي العملية أثناء الكتابة.

الإصلاحات متوفرة في PHP 8.6.0 و8.5.13 و8.4.28 و8.3.37 و8.2.36. ولم تُسجَّل حتى الآن حالات استغلال فعلي.

ما يجب فعله الآن

1. حصر التطبيقات والخوادم المعتمدة على PHP وإصداراتها ومقارنتها بالإصدارات المصححة: 8.6.0 و8.5.13 و8.4.28 و8.3.37 و8.2.36.
2. جدولة الترقية إلى إصدار مصحح عبر إدارة التغيير، مع إعطاء الأولوية للأنظمة المكشوفة على الإنترنت.
3. التحقق من تفعيل تتبع تقدم الرفع ومن استخدام تخزين الجلسات الافتراضي في ملفات، وتعطيل ما لا حاجة إليه.
4. مراجعة التطبيقات التي تخزن نصوصاً كبيرة يتحكم بها المستخدم في الجلسات، ومسارات إلغاء التسلسل غير الآمنة.
5. التأكد من تطبيق إصلاحات PHP2Shell السابقة، ومراقبة سجلات الويب بحثاً عن طلبات رفع متعددة الأجزاء غير معتادة.