أمازون: محاولات استغلال ثغرات PHP2Shell بدأت قبل صدور تصحيحات PHP بأربعة أيام



تفيد Amazon Threat Intelligence بأن محاولات استغلال ثغرتي PHP2Shell الحرجتين بدأت في 17 أكتوبر، قبل أربعة أيام من إصدار تصحيحات PHP في 21 أكتوبر. على الجهات التي تشغّل PHP التحديث فورًا.

- الثغرتان CVE-2026-109618 وCVE-2026-109619 حرجتان وتتيحان تنفيذ تعليمات برمجية عن بُعد على الأنظمة المعرّضة.
- أصدر فريق أمن PHP التصحيحات في 21 أكتوبر بعد تسرّب تفاصيل دفعه إلى تقديم موعد الإصدار.
- رصدت أمازون أولى محاولات الاستغلال في 17 أكتوبر ضد نظام فخ (honeypot) من عنوان IP مجهّل، وتنوعت الحمولات ما يشير إلى أكثر من جهة.
- ترى أمازون أن الثغرات تُستغل على نطاق واسع، مع عدم وضوح عدد الهجمات الناجحة، بينما أفاد

فريق Dataminr TRACE بعمليات مسح وأدوات استغلال غير فعّالة دون اختراقات معروفة.

- يتتبع VirusTotal أكثر من 5.1 مليون مضيف PHP مكشوف على الإنترنت.

ما الذي حدث

تفيد Amazon Threat Intelligence بأن المهاجمين بدأوا استهداف ثغرات PHP2Shell يوم السبت 17 أكتوبر، أي قبل أربعة أيام من إصدار فريق أمن PHP التصحيحات في 21 أكتوبر. الثغرتان CVE-2026-109618 وCVE-2026-109619 مصنّفتان حرجتين وتتيحان تنفيذ تعليمات برمجية عن بُعد.

ويقول فريق PHP إنه قدّم موعد الإصدار المنسّق بعد تسرّب تفاصيل على الإنترنت، منها معرّفات CVE وإرشادات التخفيف التي شُوركت مع بعض مزوّدي البنية التحتية الحرجة. ونُشرت بعض نماذج الاستغلال قبل التصحيحات، لكن الفريق أكد أنها لم تكن فعّالة.

ما المعروف عن الاستغلال

تعرّض نظام الفخ لدى أمازون لهجوم من عنوان IP مرتبط بشبكة تجهيل تجارية بينما كانت الثغرة لا تزال تحت الحظر. ولا يُعرف كيف حصل المهاجم على المعلومات. وبعد الإعلان نُشرت عدة نماذج استغلال من عناوين VPN. وقال CJ Moses، مسؤول أمن المعلومات في AWS، إن الثغرات تُستغل الآن على نطاق واسع، وإن عدد المحاولات الناجحة غير واضح، وإن على المدافعين ألا يفترضوا أن تاريخ الإعلان هو أول موعد للاستغلال.

وتقدّم Dataminr TRACE صورة أكثر تحفظًا: النشاط حتى الآن يقتصر على المسح وتحديد البصمات وأدوات استغلال غير فعّالة دون اختراقات معروفة، مع توقع ظهور أدوات فعّالة.

الأهمية

يُستخدم PHP على نطاق واسع ويدعم أنظمة إدارة محتوى شائعة مثل WordPress وDrupal وJoomla. ويتتبع VirusTotal أكثر من 5.1 مليون مضيف PHP مكشوف. ويصف مطورو PHP التصحيحات الرسمية بأنها الدفاع الدائم الوحيد، ونصح المركز الوطني للأمن السيبراني البريطاني بتحديث الخوادم فورًا أو إيقافها حتى التصحيح.

ما يجب فعله الآن

1. حصر جميع خوادم PHP المكشوفة على الإنترنت ومواقع أنظمة إدارة المحتوى المبنية على PHP، بما فيها التي يديرها أطراف ثالثة.
2. تطبيق تصحيحات PHP الرسمية للثغرتين CVE-2026-109618 وCVE-2026-109619 فورًا، وإيقاف الخوادم غير المحدّثة إن تعذّر التصحيح.
3. مراجعة سجلات خادم الويب وجدار حماية تطبيقات الويب منذ 17 أكتوبر بحثًا عن عمليات مسح أو طلبات غير معتادة أو مؤشرات على web shells.
4. التعامل مع الأنظمة المكشوفة وغير المحدّثة قبل 21 أكتوبر على أنها قد تكون مستهدفة، والتصعيد عبر إجراءات الاستجابة للحوادث عند ظهور مؤشرات.
5. مطالبة مزوّدي الاستضافة وموردي الويب بتأكيد حالة التصحيح كتابيًا.