استهداف واجهات إدارة جدران الحماية عبر ثغرات PHP في PAN-OS



أكدت Palo Alto Networks في 28 أكتوبر استغلال مهاجمين لثغرتين في PHP ضد واجهات إدارة PAN-OS المكشوفة على الإنترنت، ما يتيح تنفيذ تعليمات برمجية على خادم الويب دون مصادقة.

- أكدت Palo Alto Networks في 28 أكتوبر وجود استغلال فعلي للثغرات.
- الثغرتان هما CVE-2026-109618 وCVE-2026-109619 في PHP.
- الهدف هو واجهات إدارة PAN-OS المكشوفة على الإنترنت.
- تتيح الثغرتان تنفيذ تعليمات برمجية على خادم الويب دون مصادقة.
- يصف المصدر جدار الحماية بأنه من الأهداف المبكرة لاستغلال PHP2Shell، ويشير إلى أن الإفصاح لم يسر على نحو سلس.

ما الذي ورد في التقرير

وفق ما نشره موقع The Hacker News، كان جدار الحماية من الأهداف المبكرة لاستغلال PHP2Shell. وفي 28 أكتوبر أكدت Palo Alto Networks أن مهاجمين يستغلون ثغرتين في PHP هما **CVE-2026-109618** و**CVE-2026-109619** ضد واجهات إدارة PAN-OS التي يمكن الوصول إليها من الإنترنت.

تتيح الثغرتان لأي طرف تنفيذ تعليمات برمجية على خادم الويب دون مصادقة. ويشير المصدر كذلك إلى أن الإفصاح نفسه لم يسر كما ينبغي، دون تفاصيل إضافية في المقتطف المتاح.

لماذا يهم ذلك

كثيرًا ما يُنظر إلى أجهزة الأمن بوصفها طبقات حماية لا تطبيقات ويب. وفكرة التقرير أن واجهة إدارة جدار الحماية هي في ذاتها تطبيق ويب، وعند كشفها على الإنترنت تحمل المخاطر نفسها التي تحملها أي منظومة مواجهة للإنترنت. وتنفيذ تعليمات برمجية دون مصادقة على جهاز كهذا موقع خطير يكسبه المهاجم.

الخطوات التالية

لا يذكر المقتطف تحديثات أو إصدارات متأثرة أو إجراءات تخفيف، لذا ينبغي الرجوع إلى نشرة الجهة المصنِّعة للحصول على هذه التفاصيل. وفي الأثناء، الأولوية العملية هي التحقق مما إذا كانت أي واجهة إدارة PAN-OS لديكم متاحة من الإنترنت، والتعامل مع أي انكشاف من هذا النوع بوصفه أمرًا عاجلاً.

ما يجب فعله الآن

1. حصر جميع أجهزة PAN-OS والتحقق من إمكانية الوصول إلى واجهات إدارتها من الإنترنت.
2. تقييد الوصول الإداري بالشبكات الداخلية أو شبكات الإدارة المخصصة وعناوين المسؤولين المعتمدة.
3. مراجعة نشرة Palo Alto Networks الخاصة بـ CVE-2026-109618 وCVE-2026-109619 وتطبيق ما ورد فيها.
4. فحص سجلات واجهة الإدارة والنظام بحثًا عن نشاط غير متوقع، والتصعيد عبر مسار الاستجابة للحوادث عند وجوده.
5. إدراج واجهات إدارة جدران الحماية وأجهزة الأمن الأخرى ضمن مراجعات انكشاف تطبيقات الويب.