# Palo Alto Networks تصدر تحديثات لثغرة Fragnesia المستغلة للسيطرة على جدران PAN-OS



أصدرت Palo Alto Networks تحديثات PAN-OS لمعالجة Fragnesia) CVE-2026-46300) التي استُغلت مع PHP2Shell ضد جدران حماية واجهات إدارتها مكشوفة على الإنترنت.

- Fragnesia) CVE-2026-46300) ثغرة رفع صلاحيات في نواة Linux ضمن نظام XFRM ESP-in-TCP، وقد أُعلن عنها في مايو 2026.
- دمج المهاجمون PHP2Shell لتنفيذ الشيفرة عن بُعد مع Fragnesia لزرع webshells بصلاحيات الجذر.
- أكدت Palo Alto Networks وقوع هجمات على جدران PAN-OS التي تكون واجهات إدارتها مكشوفة على الإنترنت.
- تتوافر إصلاحات PHP2Shell لجميع إصدارات PAN-OS المدعومة منذ 30 أكتوبر، وتعالج الإصدارات الجديدة Fragnesia أيضاً.

- توصي الشركة بمنع الوصول المباشر إلى واجهة الإدارة من الإنترنت.

أعلنت Palo Alto Networks عن تحديثات PAN-OS تعالج الثغرة CVE-2026-46300 المعروفة باسم Fragnesia، وهي ثغرة في نواة Linux استُغلت للحصول على صلاحيات الجذر على جدران الحماية التابعة لها.

## ما الذي حدث

أُعلن عن Fragnesia في مايو 2026 بوصفها ثغرة رفع صلاحيات في نظام XFRM ESP-in-TCP ضمن النواة. وتتيح لمهاجم بلا صلاحيات الكتابة فوق ملفات نظام حساسة والحصول على صلاحيات الجذر.

وأفادت شركة Dream في 26 أكتوبر بأن جهة تهديد ناطقة بالصينية استخدمت ثغرات PHP2Shell الحرجة مع Fragnesia في حملة مدعومة بالذكاء الاصطناعي. ووفق التقرير جرى اختراق 25 خادماً، منها 24 جدار حماية وخادم داخلي لإدارة الجدران. أتاح PHP2Shell تنفيذ الشيفرة عن بُعد، ثم استُخدم استغلال Fragnesia لزرع webshells بصلاحيات الجذر. وفي 29 أكتوبر أكدت Palo Alto Networks أن جدران PAN-OS التي تكون واجهات إدارتها مكشوفة على الإنترنت تعرضت لهذا النوع من الهجمات.

## وضع الإصلاحات

منذ 30 أكتوبر تتوافر إصلاحات PHP2Shell لجميع إصدارات PAN-OS المدعومة، ما أغلق مسار الدخول الأولي المعروف. وتذكر الشركة أن تشغيل إصدار مُصحَّح مدرج في نشرة PHP2Shell يوفر الحماية. ومع ذلك أصدرت إصدارات جديدة لمعالجة Fragnesia ضمن الفروع 12.2 و12.1 و11.2 و11.1 و10.2، وتوصي بتطبيقها. والطريقة الوحيدة المعروفة لاستغلال Fragnesia ضد PAN-OS هي استغلال PHP2Shell أولًا عبر واجهة إدارة مكشوفة.

## كشف واجهة الإدارة

تنصح Palo Alto Networks بعدم السماح بالوصول المباشر إلى واجهة الإدارة من الويب، وأن يقتصر الوصول على شبكة الإدارة أو يمر عبر VPN.

## ما يجب فعله الآن

1. حصر جميع جدران PAN-OS والتحقق من إمكانية الوصول إلى أي واجهة إدارة من الإنترنت.
2. حصر الوصول الإداري في شبكة إدارة مخصصة أو عبر VPN.
3. التأكد من تثبيت إصلاحات PHP2Shell، ثم تطبيق إصدار PAN-OS المعالج لـ CVE-2026-46300 في الفرع المستخدم.
4. فحص الجدران التي كانت واجهات إدارتها مكشوفة بحثاً عن webshells أو تغييرات غير متوقعة في الملفات، وتصعيد أي اشتباه باختراق إلى فريق الاستجابة للحوادث.
5. توثيق حالة الانكشاف والمعالجة في سجلات إدارة الثغرات والتغيير تمهيداً لمراجعة الجهات التنظيمية.