

مجموعات فدية تستغل ثغرة CVE-2026-0257 في PAN-OS و Prisma Access رغم صدور التصحيح



أفادت Palo Alto Networks باستمرار استغلال جهات فدية للثغرة CVE-2026-0257 في PAN-OS و Prisma Access، وهي تجاوز للمصادقة يتيح اتصالات VPN غير مصرح بها. التصحيح متاح منذ مايو 2026.

- CVE-2026-0257 ثغرة تجاوز مصادقة في PAN-OS و Prisma Access بتقييم CVSS قدره 7.8.
- يمكن استغلالها لإنشاء اتصالات VPN غير مصرح بها.
- أصدرت Palo Alto Networks التصحيح في مايو 2026 وما زالت ترصد استغلالاً من جهات فدية.
- يذكر عنوان الخبر أن مجموعتي Qilin و INC تستغلانها لتجاوز المصادقة متعددة العوامل.

ما الذي ورد في الخبر

ذكرت Palo Alto Networks أنها ما زالت ترصد استغلال جهات فدية للثغرة CVE-2026-0257 التي تؤثر في PAN-OS وPrisma Access. والثغرة من نوع تجاوز المصادقة، وتبلغ درجتها 7.8 وفق مقياس CVSS، ويمكن للمهاجمين عبرها إنشاء اتصالات VPN دون تفويض.

أصدرت الشركة التصحيح في مايو 2026. ويشير عنوان التقرير إلى أن مجموعتي الفدية Qilin وINC من بين الجهات التي تستخدم الثغرة لتجاوز المصادقة متعددة العوامل.

أهمية الأمر

تُعد بوابات الوصول عن بعد نقطة دخول شائعة في عمليات الفدية. وتجاوز المصادقة في خدمة VPN يعني أن المصادقة متعددة العوامل، التي تعتمد عليها مؤسسات كثيرة كضابط رئيسي، قد لا تحمي بوابة غير محدّثة. واستمرار الاستغلال بعد أشهر من صدور التصحيح يدل على أن بعض الأجهزة لم تُحدّث بعد.

لا يتضمن المقتطف المتاح تفاصيل عن الإصدارات المتأثرة أو الضحايا أو مؤشرات الاختراق، لذا ينبغي الرجوع إلى نشرة الشركة المصنّعة لهذه التفاصيل.

الخطوات التالية

يُنصح بالتعامل مع الأمر كمهمة تحديث وتحقق لا كحالة طوارئ تستدعي إعادة تصميم. تأكدوا من أن جميع نسخ PAN-OS وPrisma Access، ومنها ما يديره أطراف ثالثة، تعمل بإصدار مُصنّح، وراجعوا سجلات VPN بحثاً عن جلسات غير متوقعة.

ما يجب فعله الآن

1. حصر جميع نسخ PAN-OS وPrisma Access، بما فيها التي يديرها مزودو الخدمة.
2. تطبيق تصحيح مايو 2026 للثغرة CVE-2026-0257 وفق نشرة Palo Alto Networks.
3. مراجعة سجلات VPN بحثاً عن اتصالات غير مصرح بها أو غير معتادة، خصوصاً قبل تاريخ التحديث.
4. عدم الاكتفاء بالمصادقة متعددة العوامل للوصول عن بعد، ومراقبة جلسات البوابة.
5. التأكد من حالة التحديث لدى مزودي الخدمات المُدارة وتوثيقها كدليل امتثال لضوابط NCA ECC وإطار SAMA CSF.