ثغرة HTTP/2 في NGINX (CVE-2026-123007) تتيح تنفيذ التعليمات دون مصادقة وإصدار نسخ مُصحَّحة



ثغرة عمرها عشر سنوات في دعم HTTP/2 بخادم NGINX، رقمها CVE-2026-123007 وتُعرف بـ"nginx2root"، قد تتيح لمهاجم دون مصادقة تنفيذ تعليمات على الخوادم المفعّل فيها HTTP/2. صدرت النسختان المُصحَّحتان 1.31.9 و1.30.7.

- الثغرة CVE-2026-123007 المسماة "nginx2root" تمس خوادم NGINX المفعّل فيها HTTP/2.
- لا يحتاج المهاجم إلى تسجيل الدخول لتنفيذ التعليمات.
- الثغرة موجودة في الشيفرة مفتوحة المصدر منذ الإصدار 1.9.5 الصادر في 22 سبتمبر 2015.
- صدرت النسختان المُصحَّحتان 1.31.9 و1.30.7.
- شركة F5 المالكة لـNGINX تؤكد أن الأثر هو تنفيذ مهاجمين لتعليمات على الخوادم.

ما الذي أُعلن عنه

توجد ثغرة في دعم HTTP/2 ضمن خادم NGINX قد تتيح لمهاجم تنفيذ تعليمات على الخادم دون مصادقة. تحمل الثغرة الرقم CVE-2026-123007 ويُطلق عليها "nginx2root"، وهي تمس الخوادم التي فُعّل فيها HTTP/2.

والثغرة موجودة في الشيفرة مفتوحة المصدر لـNGINX منذ الإصدار 1.9.5 الصادر في 22 سبتمبر 2015، أي أنها بقيت دون اكتشاف نحو عشر سنوات.

حالة الإصلاح

تتضمن النسختان 1.31.9 و1.30.7 الإصلاح، وقد صدرتا في يوم نشر الخبر. وتقول شركة F5 المالكة لـNGINX إن المهاجمين يستطيعون استغلال الثغرة لتنفيذ تعليمات. لا يورد المصدر تفاصيل تقنية إضافية مثل حالة الاستغلال الفعلي أو حلول مؤقتة، لذا ينبغي الرجوع مباشرة إلى نشرات F5 وNGINX.

الأثر على الجهات الخاضعة للتنظيم

يُستخدم NGINX عادةً كخادم ويب أو وكيل عكسي أو موزّع أحمال، وغالباً على حدود الشبكة ومكشوفاً للإنترنت. وثغرة لا تتطلب بيانات اعتماد وتمس بروتوكولًا مفعّلًا على نطاق واسع تستحق معالجة عاجلة. وأول الخطوات معرفة أماكن تشغيل NGINX، بما في ذلك داخل الأجهزة المتخصصة والحاويات والمنتجات الخارجية، وهل HTTP/2 مفعّل عليه.

ويُنفَّذ التحديث وفق إجراءات التغيير الطارئ المعتمدة، مع ترتيب الأنظمة المتأثرة بحسب درجة انكشافها وأهميتها للأعمال.

ما يجب فعله الآن

1. حصر جميع نسخ NGINX، بما فيها المضمّنة في الأجهزة المتخصصة والحاويات ومنتجات الموردين.
2. تحديد النسخ المفعّل فيها HTTP/2 بدءاً بالمكشوفة للإنترنت.
3. الترقية إلى NGINX 1.31.9 أو 1.30.7 أو تطبيق الإصلاح المكافئ من المورد عبر إجراء التغيير الطارئ.
4. مطالبة الموردين الذين تتضمن منتجاتهم NGINX بإفادتكم بحالة التحديث وموعده.
5. مراجعة سجلات خوادم الويب والوكلاء بحثاً عن نشاط غير معتاد وتسجيل الثغرة في سجل إدارة الثغرات.