CERT-EU: خمس ثغرات حرجة في NGINX تتيح تنفيذ تعليمات برمجية عن بُعد دون مصادقة



أعلنت F5 عن خمس ثغرات في NGINX بدرجة CVSS تبلغ 8.1 لكل منها، تتيح لمهاجم غير موثّق تنفيذ تعليمات برمجية بصلاحيات عملية العامل. لم يُبلَّغ عن استغلال فعلي، وتوصي CERT-EU بالتحديث العاجل بدءًا بالأنظمة المكشوفة للإنترنت.

- خمس ثغرات في NGINX (CVE-2026-123007 وCVE-2026-123633 وCVE-2026-121810 وCVE-2026-123634 وCVE-2026-113425) تبلغ درجة CVSS لكل منها 8.1.
- يمكن أن تؤدي جميعها إلى تنفيذ تعليمات برمجية دون مصادقة بصلاحيات عملية العامل في NGINX.
- نجح باحثون في إثبات إمكانية استغلال CVE-2026-123007، ولم يُبلَّغ حتى الآن عن استغلال فعلي.
- المتأثر: NGINX Open Source الإصدارات mainline من 1.9.5 إلى 1.31.8، وإصدارات stable ضمن

x.1.30، وNGINX Plus بما فيها R34 وR35 وR36 وإصدارات x.37 عدة.

- تعطيل HTTP/2 على المنافذ المكشوفة يخفف CVE-2026-123007 وCVE-2026-123633 عند تعذّر التحديث الفوري.

ما الذي أُعلن

في 18 نوفمبر 2026 نشرت F5 نشرة تتناول خمس ثغرات في NGINX، ولخّصها فريق CERT-EU في النشرة 022-2026. تبلغ درجة كل ثغرة 8.1 وفق CVSS، ويمكن لكل منها أن تتيح لمهاجم عن بُعد دون مصادقة تنفيذ تعليمات برمجية بصلاحيات عملية العامل في NGINX.

يعتمد الاستغلال على إعدادات محددة. فالثغرة CVE-2026-123007 فيض أعداد صحيحة في التحكم بتدفق HTTP/2 ويكفي لاستغلالها تفعيل HTTP/2 على منفذ استماع. أما CVE-2026-123633 وCVE-2026-121810 فهما ثغرتا استخدام بعد التحرير (use-after-free) ترتبطان باتصالات HTTP/2 وQUIC) HTTP/3) مع التمرير إلى خادم upstream. وتتعلق CVE-2026-123634 بقائمة انتظار محلّل DNS، وCVE-2026-113425 بمصادقة وكيل البريد عبر auth_http.

أثبت باحثون إمكانية استغلال CVE-2026-123007، ولم يُبلَّغ حتى الآن عن استغلال فعلي.

المنتجات المتأثرة

- NGINX Open Source (mainline) من 1.9.5 إلى 1.31.8 بحسب الثغرة
- NGINX Open Source (stable) ضمن x.1.30 بما فيها 1.30.6
- NGINX Plus من 37.0.0 إلى 37.0.7.1 ومن 37.1.0 إلى 37.2.0.1، إضافة إلى R34 وR35 وR36

تتوفر الإصدارات المعالَجة في نشرة F5.

الاستجابة الموصى بها

توصي CERT-EU بالتحديث في أقرب وقت، بدءًا بالنسخ المكشوفة للإنترنت. وإن تعذّر ذلك فورًا، فإن إزالة http2 من توجيهات listen أو ضبط http2 off; يخفف CVE-2026-123007 وCVE-2026-123633 فقط.

ولتقييم احتمال الاختراق، يُراقَب سجل الأخطاء لرصد خروج عمليات العامل بإشارة. وهذا مؤشر على محاولات استغلال لا على تنفيذ فعلي مؤكد، لذا يلزم فحص سجلات إنشاء العمليات أيضًا.

ما يجب فعله الآن

1. حصر جميع نسخ NGINX Open Source وNGINX Plus بما فيها المضمّنة في الأجهزة ومقارنة إصداراتها بنشرة F5.
2. تطبيق الإصدارات المعالَجة الواردة في نشرة F5 بدءًا بالنسخ المكشوفة للإنترنت.
3. عند تعذّر التحديث الفوري، تعطيل HTTP/2 على المنافذ المكشوفة لتخفيف CVE-2026-123007 وCVE-2026-123633 وتوثيق الاستثناء.
4. مراجعة الإعدادات المتعلقة بـ HTTP/3 ومحلّل DNS مع proxy_pass المبني من بيانات الطلب ووكيل

البريد مع auth_http لتقدير التعرض للثغرات الثلاث الأخرى.

5. البحث في سجلات أخطاء NGINX عن خروج عمليات العامل بإشارة، وفحص سجلات إنشاء العمليات على أي خادم تظهر فيه.
6. متابعة المعالجة ضمن إدارة الثغرات بما يتوافق مع متطلبات إدارة التحديثات في ضوابط NCA ECC.