F5 تصدر تصحيحات لخمس ثغرات حرجة في NGINX عُرفت باسم NGINX2Root



أصدرت F5 تصحيحات لخمس ثغرات حرجة في NGINX قد تتيح تنفيذ التعليمات عن بُعد في ظروف معينة. لا يوجد استغلال فعلي معروف، لكن يتوفر استغلال تجريبي علني لإحداها.

- خمس ثغرات حرجة في NGINX سمّاها باحثو Xint باسم NGINX2Root قد تتيح تنفيذ التعليمات عن بُعد بصلاحيات عملية العامل إذا عُطّل ASLR أو جرى تجاوزه.
- يتوفر استغلال تجريبي علني للثغرة CVE-2026-123007، وتصفه Rapid7 بأنه مقيّد، إذ يحتاج نحو 128 غيغابايت من حركة HTTP/2 وتجاوز ASLR.
- لا يوجد استغلال فعلي معروف، ولم تكن أي منها في كتالوج KEV التابع لـCISA حتى 19 نوفمبر.
- الوصول إلى صلاحيات root يتطلب ثغرة سادسة في نواة لينكس (SCTP) لا تحمل رقم CVE حتى 18 نوفمبر ولم تُصحَّح بعد.
- الإصدارات المصححة: NGINX Open Source بالنسختين 1.30.7 و1.31.9، وNGINX Plus بالنسختين

> 37.0.8.1 و37.3.0.1، مع لزوم إعادة التشغيل بعد الترقية.

أصدرت F5 تصحيحات لخمس ثغرات حرجة في NGINX سمّاها باحثو Xint باسم NGINX2Root، وقد تتيح في ظروف معينة تنفيذ التعليمات عن بُعد. وكانت ثغرتان منها، CVE-2026-123633 وCVE-2026-123007، قد أبلغت عنهما بشكل مستقل فرق بحثية أخرى.

ما الذي يتأثر

ثلاث من الثغرات من نوع use-after-free ترتبط بـHTTP/2 ومحلّل DNS وHTTP/3 عبر QUIC، ورابعة في مسار auth_http ضمن وكيل البريد. أما الخامسة CVE-2026-123007 فهي تدفق عددي سالب في التحكم بتدفق HTTP/2 قد يُسقط عملية العامل وقد يتيح تنفيذ التعليمات. وإذا كان ASLR معطلًا أو جرى تجاوزه، فبإمكان أي منها تنفيذ التعليمات بصلاحيات عملية العامل في NGINX. أما الوصول إلى root فيتطلب ثغرة سادسة في شيفرة SCTP بنواة لينكس، لم يكن لها رقم CVE ولا تصحيح حتى 18 نوفمبر.

حالة الاستغلال

لا يوجد استغلال فعلي معروف. ويتوفر استغلال تجريبي علني للثغرة CVE-2026-123007 تصفه Rapid7 بأنه مقيّد: يعتمد على روتين في glibc لبنى x86-64، ويحتاج نحو 128 غيغابايت من حركة HTTP/2، ويجب أن يستعيد عناوين الذاكرة الكومة لتجاوز ASLR. وتشير Tenable إلى أن نجاحه مستبعد خلف وكلاء تنهي اتصالات HTTP/2 أو على اتصالات بطيئة. ولدى Xint وWiz استغلالات للثغرات الخمس لكنهما لم تنشراها.

المعالجة

الترقية أفضل من التدابير المؤقتة. الإصدارات المصححة هي NGINX Open Source بالنسختين 1.30.7 و1.31.9، وNGINX Plus بالنسختين 37.0.8.1 و37.3.0.1. ويجب إعادة تشغيل NGINX بعد ذلك لأن إعادة تحميل الإعدادات لا تستبدل الملف التنفيذي العامل. ومستخدمو حزم التوزيعات عليهم التحقق من التصحيحات المنقولة. كما يدخل NGINX في منتجات F5 أخرى، بعضها صدرت له تحديثات وبعضها ما زال قيد العمل.

ما يجب فعله الآن

1. حصر جميع نسخ NGINX، بما فيها المضمّنة في NGINX Instance Manager وIngress Controller وGateway Fabric، وإعطاء الأولوية للمكشوفة على الإنترنت.
2. الترقية إلى الإصدارات المصححة وإعادة تشغيل الخدمة، وعدم الاكتفاء بإعادة تحميل الإعدادات.
3. عند استخدام حزم التوزيعات، التأكد من المورّد بأن التصحيحات نُقلت إلى الإصدارات المثبّتة.
4. التحقق من تفعيل ASLR على الخوادم التي تشغّل NGINX ومتابعة صدور تصحيح SCTP في نواة لينكس.
5. الاطلاع على إرشادات Xint للتحقق من أي نشاط محتمل مرتبط بالثغرة CVE-2026-123007 على الخوادم المكشوفة.
6. تقليص الأنظمة المكشوفة للإنترنت، وأتمتة التصحيح، وتقييد ما يمكن لكل تطبيق الوصول إليه.