

NGINX تصدر تحديثات لمعالجة خمس ثغرات تشمل احتمال تنفيذ تعليمات برمجية عن بُعد وتزوير جلسات TLS



أصدرت NGINX الإصدارين 1.30.6 و1.31.7 في 14 أكتوبر لمعالجة خمس ثغرات أمنية، منها ثلاث ثغرات في الذاكرة قد تتيح تنفيذ تعليمات برمجية عن بُعد وثغرة في TLS تسمح بتزوير الجلسات.

- إصدار NGINX 1.30.6 و1.31.7 في 14 أكتوبر 2025 لمعالجة خمس ثغرات أمنية
- ثلاث ثغرات متعلقة بالذاكرة قد تتسبب في تعطل عمليات العمل أو تتيح تنفيذ تعليمات برمجية عن بُعد في ظروف محددة
- ثغرة في TLS تسمح للمهاجمين بتزوير الجلسات وربما تجاوز التحقق من شهادات العميل
- إحدى الثغرات موجودة في جميع إصدارات NGINX منذ مايو 2005
- جميع ثغرات الذاكرة الثلاث تتطلب إعدادات خادم محددة لاستغلالها

نظرة عامة على الثغرات

أصدرت شركة F5 المالكة لـ NGINX إصدارين محدثين في 14 أكتوبر 2025 لمعالجة خمس ثغرات أمنية تؤثر على برنامج خادم الويب والوكيل العكسي واسع الانتشار. تعالج إصدارات NGINX 1.30.6 و1.31.7 ثلاث ثغرات متعلقة بالذاكرة قد تتسبب في تعطل عمليات العمل أو، في ظروف معينة، قد تسمح للمهاجم بتنفيذ تعليمات برمجية عشوائية. تتطلب كل من ثغرات الذاكرة هذه إعدادات خادم محددة لاستغلالها.

تؤثر الثغرة الرابعة على **معالجة جلسات TLS** وتسمح للمهاجم بتزوير جلسة، مما قد يتيح تجاوز ضوابط التحقق من شهادات العميل. والجدير بالذكر أن إحدى الثغرات المعالجة كانت موجودة في جميع إصدارات NGINX منذ مايو 2005، مما يمثل فترة تعرض تقارب عقدين من الزمن.

المخاطر على المؤسسات الخاضعة للتنظيم

يستخدم NGINX بشكل شائع في البنية التحتية الأمامية للويب وبوابات API وطبقات موازنة الأحمال عبر قطاعات الخدمات المالية والرعاية الصحية والحكومة في المملكة. يمثل احتمال تنفيذ تعليمات برمجية عن بُعد، حتى عند الاعتماد على الإعدادات، خطراً جوهرياً على سرية وسلامة وتوافر الخدمات الحرجة. تثير ثغرة تزوير جلسات TLS قلقاً خاصاً للمؤسسات التي تعتمد على مصادقة TLS المتبادلة لفرض ضوابط الوصول للتطبيقات أو واجهات API الحساسة.

الاستجابة الفورية

يجب على المؤسسات جرد جميع عمليات نشر NGINX وإعطاء الأولوية للحالات المواجهة للإنترنت والدرجة للأعمال وجدولة التحديث إلى أحدث الإصدارات المستقرة. يجب أن تؤكد مراجعات الإعدادات ما إذا كانت الإعدادات المحددة التي تمكّن استغلال ثغرات الذاكرة قيد الاستخدام، كما يجب التحقق من آليات مصادقة شهادات عميل TLS.

ما يجب فعله الآن

1. جرد جميع عمليات نشر NGINX عبر بيئات الإنتاج والتجهيز والتطوير
2. إعطاء الأولوية لتحديث حالات NGINX المواجهة للإنترنت وتلك التي تتعامل مع البيانات الحساسة أو المصادقة
3. الترقية إلى إصدار NGINX 1.30.6 أو 1.31.7 وفقاً لإجراءات إدارة التغيير
4. مراجعة إعدادات NGINX لتحديد الإعدادات التي قد تمكّن من استغلال ثغرات الذاكرة
5. التحقق من آليات مصادقة شهادات عميل TLS وسياسات التحكم في الوصول
6. مراقبة سجلات أخطاء NGINX وسجلات الأحداث الأمنية للكشف عن تعطل غير طبيعي لعمليات العمل أو تجاوز المصادقة