

F5 تصدر تحديثات طارئة لثغرات حرجية في NGINX تتيح تنفيذ التعليمات البرمجية



أصدرت F5 تحديثات أمنية طارئة لمعالجة ثلاث ثغرات حرجية في NGINX تتيح تنفيذ تعليمات برمجية عن بُعد وهجمات حجب الخدمة على الأنظمة ذات الإعدادات غير الافتراضية.

- ثلاث ثغرات حرجية (CVE-2026-15176 و CVE-2026-97205 و CVE-2026-93479) تؤثر على مكونات خادم الويب NGINX
- يمكن للمهاجمين عن بُعد استغلال الثغرات دون امتيازات لتنفيذ تعليمات برمجية أو شن هجمات حجب خدمة على الإعدادات غير الافتراضية
- تتوفر تحديثات لمنتجات NGINX Plus و NGINX Open Source و NGINX Ingress Controller و NGINX Instance Manager و NGINX Gateway Fabric
- تتوفر حلول تخفيف مؤقتة للمؤسسات غير القادرة على تطبيق التحديثات فوراً
- منتجات F5 كانت هدفاً للجهاز المهددة في السنوات الأخيرة، مع استغلال ثماني ثغرات في

تفاصيل الثغرات

أصدرت F5 تحديثات أمنية طارئة لمعالجة ثغرات متعددة حرجية في منصة خادم الويب NGINX. تحمل ثلاث ثغرات تصنيف خطورة حرج: اثنان في مكون (CVE-2026-15176 ngx_http_v3_module و CVE-2026-97205) وواحدة في توجيهه (CVE-2026-93479 NGINX map). يمكن للمهاجمين عن بُعد دون مصادقة استغلال هذه الثغرات على الأنظمة التي تعمل بإعدادات غير افتراضية.

يؤدي الاستغلال الناجح إلى حدوث فيض في المخزن المؤقت أو استخدام بعد التحرير في عملية عامل NGINX، مما يتسبب في تعطل النظام أو إعادة تشغيل قسرية. والأخطر من ذلك، قد يتمكن المهاجمون من تنفيذ تعليمات برمجية تعسفية على الأنظمة التي تم تعطيل عشوائية تخطيط مساحة العنوان فيها أو عندما يمكن تجاوز حماية ASLR.

المنتجات المتأثرة وإجراءات التخفيف

تؤثر الثغرات على منتجات برمجيات NGINX المتعددة بما في ذلك NGINX Plus و NGINX Open Source و NGINX. أصدرت F5 تحديثات لجميع الإصدارات المتأثرة.

بالنسبة للمؤسسات غير القادرة على تطبيق التحديثات فوراً، نشرت F5 إجراءات تخفيف مؤقتة. يمكن تخفيف CVE-2026-15176 بتجنب توجيهه alias في كتل الموقع ومتغير request_filename\$. يمكن تقليل مخاطر CVE-2026-97205 بتعطيل الإدخال والإخراج غير المتزامن للملفات أو Server Side Includes. يمكن معالجة CVE-2026-93479 باستخدام الالتقاطات المسماة بدلاً من غير المسماة وتقييد نطاقها.

سياق التهديد

رغم أن F5 لم تؤكد الاستغلال النشط لهذه الثغرات المحددة، فإن منتجات الشركة كانت أهدافاً متكررة. منذ نوفمبر 2021، تم تصنيف ثماني ثغرات في F5 كمستغلة بنشاط، مع استخدام أربع منها في حملات برمجيات الفدية. استغل الفاعلون المهددون سابقاً ثغرات F5 لاختراق الشبكات ورسم خرائط البنية التحتية واختطاف الأجهزة وسرقة بيانات حساسة. في أغسطس 2025، اخترق فاعلون مدعومون من دول أنظمة F5 وسرقوا شفرة مصدريه ومعلومات عن ثغرات BIG-IP غير المعلنة.

ما يجب فعله الآن

1. تحديد جميع نشر NGINX عبر بنيتك التحتية، بما في ذلك NGINX Plus و Open Source و Ingress و Instance Manager و Gateway Fabric و Controller.
2. تطبيق تحديثات F5 الأمنية فوراً على جميع أنظمة NGINX المتأثرة، مع إعطاء الأولوية للخوادم المواجهة للإنترنت والبنية التحتية الحرجة.
3. للأنظمة التي لا يمكن تحديثها فوراً، تنفيذ إجراءات التخفيف المؤقتة التي نشرتها F5 لكل ثغرة.
4. مراجعة إعدادات NGINX لتحديد الإعدادات غير الافتراضية التي قد تزيد من التعرض لهذه الثغرات.

5. مراقبة أنظمة NGINX بحثاً عن أعطال أو عمليات إعادة تشغيل غير عادية أو سلوك مريب لعملية العامل
قد يشير إلى محاولات استغلال

6. توثيق حالة التحديث وإجراءات التخفيف لإعداد التقارير الامتثالية للهيئة الوطنية للأمن السيبراني أو
مؤسسة النقد العربي السعودي حسب الاقتضاء