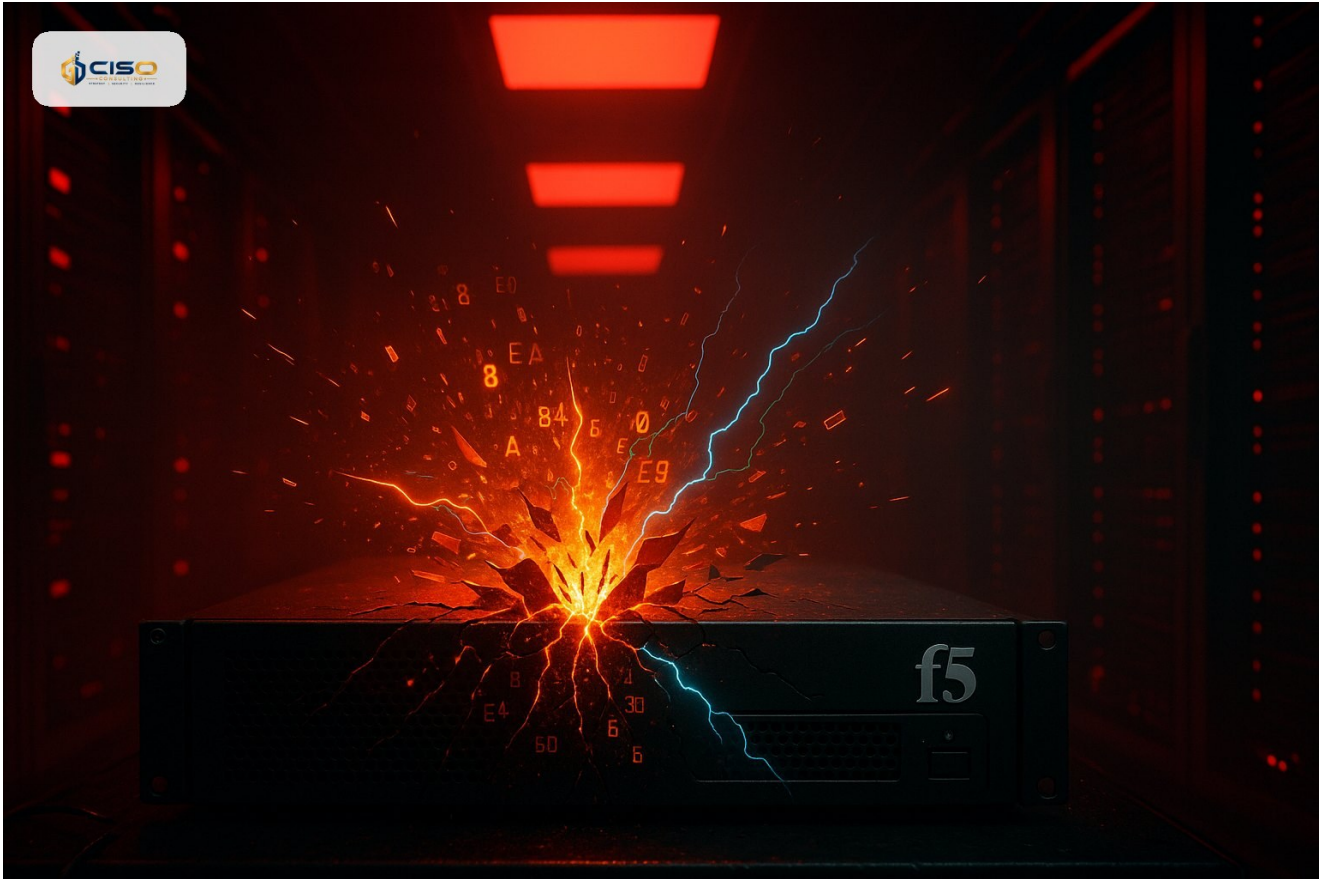


ثغرة تجاوز سعة الذاكرة في F5 BIG-IP APM تتيح تنفيذ تعليمات برمجية عن بُعد



يحتوي F5 BIG-IP APM على ثغرة تجاوز سعة ذاكرة مؤقتة تتيح تنفيذ تعليمات برمجية عن بُعد دون مصادقة عند تكوين سياسة الوصول وملف OAuth على خادم افتراضي.

- ثغرة تجاوز سعة ذاكرة مؤقتة في F5 BIG-IP APM (CVE-2026-94127)
- يمكن للمهاجمين غير المصادقين تنفيذ تعليمات برمجية عن بُعد على الأنظمة المعرضة للخطر
- تؤثر الثغرة على الأنظمة التي تحتوي على سياسة وصول وملف OAuth مكوّنين على خوادم افتراضية
- يجب تطبيق تدابير الحماية من المورّد فوراً أو إيقاف الخدمات المتأثرة
- تتطلب الأصول المعرضة للإنترنت تقييماً ومعالجة ذات أولوية

نظرة عامة على الثغرة

كشفت F5 Networks عن ثغرة تجاوز سعة ذاكرة مؤقتة تحمل الرمز CVE-2026-94127 تؤثر على مدير سياسة الوصول (BIG-IP APM). تتيح هذه الثغرة للمهاجمين غير المصادقين تنفيذ تعليمات برمجية تعسفية عن بُعد على الأنظمة المعرضة للخطر. تظهر الثغرة عند تكوين سياسة وصول وملف OAuth على خادم افتراضي، وهو نمط نشر شائع في بنى المصادقة والتفويض المؤسسية.

تتبع خطورة هذه الثغرة من إمكانية استغلالها عن بُعد دون مصادقة واحتمال اختراق النظام بالكامل من خلال تنفيذ التعليمات البرمجية. تواجه المؤسسات التي تستخدم BIG-IP APM لتوصيل التطبيقات أو إدارة الوصول أو اتحاد الهوية خطراً فوراً إذا بقيت الأنظمة دون تصحيح.

المخاطر على المؤسسات السعودية

تنشر المؤسسات الخاضعة للتنظيم في المملكة عادةً حلول F5 BIG-IP لتوصيل التطبيقات الآمن والتحكم في الوصول إلى الأنظمة الحيوية. يجب على المؤسسات المالية ومقدمي الرعاية الصحية والجهات الحكومية التي تستخدم BIG-IP APM مع تكوينات OAuth معاملة هذا الأمر كحادث ذي أولوية يتطلب إجراءً فوراً. تمثل عمليات النشر المواجهة للإنترنت أعلى مستوى خطر وتتطلب اهتماماً عاجلاً.

إرشادات المعالجة

يجب على المؤسسات تطبيق تدابير الحماية المقدمة من المورد دون تأخير. حيثما تكون التصحيحات أو الحلول البديلة غير متاحة، ينبغي عزل الخدمات المتأثرة عن الشبكات غير الموثوقة أو إيقافها حتى يمكن تنفيذ تكوينات آمنة. يجب مراجعة جرد الأصول لتحديد جميع عمليات نشر BIG-IP APM، مع التركيز بشكل خاص على الحالات المعرضة للإنترنت وتلك التي تتعامل مع المصادقة للأنظمة الحساسة. يجب أن تتحقق مراجعات التكوين مما إذا كانت سياسات الوصول وملفات OAuth نشطة على الخوادم الافتراضية.

ما يجب فعله الآن

1. حدد جميع عمليات نشر F5 BIG-IP APM عبر بنيتك التحتية، مع إعطاء الأولوية للحالات المواجهة للإنترنت
2. تحقق من الأنظمة التي تحتوي على سياسة وصول وملف OAuth مكوّنين على خوادم افتراضية
3. طبّق التصحيحات أو تدابير الحماية المقدمة من المورد فوراً وفقاً لنشرات F5 الأمنية
4. اعزل الأنظمة المعرضة للخطر عن الشبكات غير الموثوقة أو أوقف الخدمات إذا كانت التصحيحات غير متاحة
5. راجع سجلات الوصول ونشاط النظام للبحث عن مؤشرات الاستغلال أو محاولات الوصول غير المصرح بها
6. حدّث إجراءات الاستجابة للحوادث لتشمل هذه الثغرة في أنشطة البحث عن التهديدات