ثغرة حرجة في F5 BIG-IP APM (CVE-2026-94127) قيد الاستغلال الفعلي



أكدت F5 استغلال الثغرة (CVSS 9.8) CVE-2026-94127 في BIG-IP APM، وهي تجاوز سعة في الذاكرة يتيح تنفيذ تعليمات عن بُعد دون مصادقة. ويوصي CERT-EU بالتصحيح العاجل وفحص الاختراق.

- الثغرة CVE-2026-94127 بدرجة CVSS تبلغ 9.8، وهي تجاوز سعة في الذاكرة (heap) يتيح تنفيذ تعليمات عن بُعد دون مصادقة.
- أكدت F5 وجود استغلال فعلي عند نشر نشرتها في 22 سبتمبر 2026.
- النسخ المتأثرة من BIG-IP APM: 17.1.0–17.1.3 و17.5.0–17.5.1 و21.1.0 عند إعداد سياسة وصول وملف OAuth على خادم افتراضي.
- يتوفر تخفيف قائم على iRule عبر دعم F5 إن تعذّر التصحيح فورًا.
- المؤشر الأبرز: إخفاقات OAuth متكررة ثم أوامر مشبوهة ثم SIGABRT في TMM.

ما الذي حدث

في 22 سبتمبر 2026 نشرت F5 نشرة بشأن ثغرة حرجة في BIG-IP APM وأكدت أنها تُستغل فعليًا. كما أصدر CERT-EU نشرته الخاصة داعيًا إلى اتخاذ الإجراءات في أقرب وقت.

الثغرة **CVE-2026-94127** بدرجة CVSS تبلغ 9.8، وهي تجاوز سعة في ذاكرة heap يتيح لمهاجم غير مصادَق تنفيذ تعليمات برمجية عن بُعد على الجهاز المتأثر.

الجهات المتأثرة

تشمل النسخ المتأثرة من BIG-IP APM: من 17.1.0 إلى 17.1.3، ومن 17.5.0 إلى 17.5.1، والنسخة 21.1.0، وذلك فقط عند إعداد سياسة وصول وملف OAuth على خادم افتراضي.

فحص الاختراق

يشير CERT-EU إلى مؤشرات قدمتها الشركة المصنِّعة. والتركيب الذي يستدعي مراجعة بشرية هو: إخفاقات مصادقة OAuth متعددة، تليها أوامر مشبوهة، ثم SIGABRT في TMM بوقت قريب.

- راجع /var/log/apm بحثًا عن إخفاقات OAuth متكررة، خصوصًا 10 مرات أو أكثر من عنوان IP واحد خلال فترة قصيرة.
- افحص إحصاءات إخفاق OAuth لرصد ارتفاع غير مبرر في total_failed.
- راجع /var/log/audit في الأوقات نفسها بحثًا عن أوامر مشبوهة.
- حقّق في ملفات TMM core؛ وجودها وحده ليس مؤشرًا، لكن F5 رصدت دخول TMM في حلقة تدفع SOD إلى إرسال SIGABRT.

التخفيف

إذا تعذّر تطبيق الحزمة التصحيحية فورًا، توفر F5 تخفيفًا قائمًا على iRule للخادم الافتراضي المتأثر، ويمكن الحصول عليه بالتواصل مع دعم F5.

ما يجب فعله الآن

1. حصر جميع أنظمة BIG-IP APM والتحقق من تشغيلها نسخة متأثرة مع سياسة وصول وملف OAuth على خادم افتراضي.
2. حفظ الأدلة الجنائية (السجلات وسجلات التدقيق وملفات TMM core) قبل إجراء أي تغيير.
3. تطبيق الحزمة التصحيحية المناسبة من F5 بشكل عاجل.
4. طلب التخفيف القائم على iRule من دعم F5 إذا تأخر التصحيح.
5. مراجعة /var/log/apm و/var/log/audit وإحصاءات إخفاق OAuth بحثًا عن مؤشرات الاختراق.
6. عند ظهور أي دليل على اختراق، بدء إجراءات الاستجابة للحوادث وإبلاغ الأطراف المعنية وفق المتطلبات الداخلية والتنظيمية.