AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-94127

Heap-Overflow im OAuth-Server: F5 BIG-IP APM ohne Anmeldung übernehmbar.

BIG-IP APM enthält einen Heap-Overflow in der OAuth-Verarbeitung: Ist APM als OAuth Authorization Server konfiguriert – also mit Access-Policy und OAuth-Profil auf einem Virtual Server –, kann ein Angreifer mit präpariertem Datenverkehr ohne Anmeldung eigenen Code auf dem System ausführen. F5 hat die Lücke am 22. September 2026 veröffentlicht und bestätigt, dass sie bereits ausgenutzt wird. Behoben ist sie vorerst nur über Engineering-Hotfixes; bis zu deren Einspielung stellt F5 eine iRule über den Support bereit. CISA führt sie seit demselben Tag im KEV-Katalog – mit drei Tagen Frist und forensischer Triage-Pflicht.

Geschäftsrisiko: Übernahme des Zugangs-Gateways, über das sich Nutzer und Anwendungen anmelden – mit Zugriff auf Sitzungen, Tokens und nachgelagerte Anwendungen, als Ausgangspunkt für Lateral Movement, Datenabfluss und Erpressung; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist in diesem Fall wahrscheinlich.

9,3 / 10

KRITISCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` – aus dem Netz, ohne Rechte, ohne besondere Voraussetzungen und ohne Zutun eines Nutzers, mit voller Wirkung auf das System. Basiswert 9,3 = CVSS 4.0 von F5 als CNA (von NVD übernommen); nach CVSS 3.1 liegt er bei 9,8 – beides KRITISCH.

AUSGENUTZT SEIT
spätestens September 2026

BETROFFEN
BIG-IP APM 21.1.0 · 17.5 · 17.1
nur als OAuth-Server

HANDLUNGSBEDARF
Sofort

Das Wichtigste in 60 Sekunden.

9,3 · KRITISCH
CVSS 4.0 Basiswert (F5)

Unauth. RCE
APM als OAuth Authorization Server

Aktiv
ausgenutzt · CISA KEV · Frist 25.09.2026

Nur Hotfix
Engineering-Hotfix · iRule über F5-Support

Die Ursache: Arbeitet BIG-IP APM als **OAuth Authorization Server**, verarbeitet das Traffic-Management-Modul (TMM) die OAuth-Anfragen auf der Datenebene. Präparierter Datenverkehr an einen solchen Virtual Server löst einen Heap-Overflow aus (**CWE-122**) – und darüber Codeausführung, **ohne Zugangsdaten und ohne Nutzerinteraktion**, auch im Appliance-Modus. Die Verwaltungsoberfläche ist nicht beteiligt. Reine OAuth-Client- oder Resource-Server-Setups sind laut F5 nicht betroffen. F5 hat die Lücke intern gefunden.

ANGRIFFSKETTE

01 **Ziel erreichbar** – Virtual Server mit APM-Access-Policy und OAuth-Server-Profil

02 **Präparierter Verkehr** – wiederholte OAuth-Anfragen lösen den Heap-Overflow im TMM aus

03 **Codeausführung** – ohne Anmeldung, Befehle auf dem BIG-IP-System

04 **Ausbreitung** – Zugriff auf Sitzungen, Tokens und die dahinterliegenden Anwendungen

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
BIG-IP APM 21.x	21.1.0	Hotfix-BIGIP-21.1.0.2.0.30.22-ENG
BIG-IP APM 17.5	17.5.0 – 17.5.1	Hotfix-BIGIP-17.5.1.9.0.160.12-ENG
BIG-IP APM 17.1	17.1.0 – 17.1.3	Hotfix-BIGIP-17.1.3.5.0.41.14-ENG
Übrige F5-Produkte	nicht betroffen	keine Maßnahme nötig

Angreifbar nur mit APM als **OAuth Authorization Server**. Die Fixes sind **Engineering-Hotfixes** über F5 Downloads (K000163302), noch kein regulärer Release. Versionen jenseits des Supports (EoTS) hat F5 nicht bewertet – als verwundbar behandeln. Stände gegen K000162605 abgleichen.

Regulatorischer Hinweis: Ein übernommenes Zugangs-Gateway mit Zugriff auf Sitzungen und Tokens ist in der Regel eine meldepflichtige Verletzung – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung, Forensik und Dokumentation.

ZEITACHSE

22.09.2026
F5 veröffentlicht K000162605 – Ausnutzung bestätigt

22.09.2026
Aufnahme in CISA KEV · Triage-Pflicht

23.09.2026
Advisory aktualisiert · NVD-Analyse

25.09.2026
Ablauf der CISA-Frist (US-Behörden)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Mitigation vor Patch, Triage vor Entwarnung.

01 Betroffenheit feststellen

Version aller BIG-IP-Systeme mit APM erheben (betroffen: 21.1.0, 17.5.0 – 17.5.1, 17.1.0 – 17.1.3). Dann prüfen, ob APM irgendwo als **OAuth Authorization Server** arbeitet, also ein OAuth-Server-Profil zusammen mit einer Access-Policy an einem Virtual Server hängt. Nur diese Kombination ist angreifbar – reine OAuth-Client-Setups nicht.

```
tmsh show sys version
```

02 Sofort mitigieren (vor dem Patch)

F5 stellt eine **iRule** bereit, die auf den betroffenen APM-Virtual-Server gelegt wird – erhältlich ausschließlich über ein Ticket beim F5-Support. CISA empfiehlt ausdrücklich, zuerst diese iRule einzusetzen, dann die forensische Triage durchzuführen und erst danach zu patchen. Bis dahin den Zugriff auf den OAuth-Virtual-Server so weit wie betrieblich möglich einschränken.

03 Patchen

Den Engineering-Hotfix des eigenen Zweigs von F5 Downloads installieren: `Hotfix-BIGIP-21.1.0.2.0.30.22-ENG`, `Hotfix-BIGIP-17.5.1.9.0.160.12-ENG` bzw. `Hotfix-BIGIP-17.1.3.5.0.41.14-ENG`. Die Hotfixes enthalten zugleich alle Korrekturen der Hardened Releases 2. Vorher UCS-Sicherung ziehen, HA-Paare nach F5-Upgrade-Pfad aktualisieren und auf den regulären Maintenance-Release umsteigen, sobald er erscheint.

04 Kompromittierung ausschließen

Der Patch schließt die Tür – er wirft niemanden hinaus, der schon drin ist. F5 nennt drei Indikatoren, die in kurzem zeitlichem Abstand auftreten: gehäufte OAuth-Fehler in `/var/log/apm`, verdächtige Befehle im Audit-Log `/var/log/audit` und kurz darauf ein TMM-Absturz (SIGABRT, Core-File). Den Zähler der fehlgeschlagenen OAuth-Anfragen auf unerklärliche Anstiege prüfen.

```
tmctl global_oauth_stat -s
total_requests,total_userinfo_requests,total_failed
```

05 Bei Verdacht: Gateway als kompromittiert behandeln

Bei jedem Treffer: Beweise sichern (Logs, Core-Files, UCS), bevor das System neu aufgesetzt wird. Auf dem Gerät hinterlegte Schlüssel, Zertifikate und Client-Secrets der OAuth-Profile erneuern, ausgestellte Tokens widerrufen und die Konfiguration auf fremde Einträge prüfen – dokumentiert für eine etwaige Meldung.

Kompromittierungs-Indikatoren (IoCs)

OAUTH-FEHLER (/VAR/LOG/APM)

`01990004:3` … Request UserInfo … failed `Error Code (invalid_token)` – ab ≥ 10 je Log, v. a. von einer IP

AUDIT-LOG (/VAR/LOG/AUDIT)

Verdächtige Befehle im zeitlichen Umfeld der gehäuften OAuth-Fehler

SYSTEM

TMM-Absturz per `SIGABRT` (SOD-Daemon) mit Core-File,
Anstieg von `total_failed` in `global_oauth_stat`

Zur Einordnung: Die Indikatoren stammen aus dem F5-Advisory K000162605. F5 betont, dass jeder einzelne für sich normal sein kann – erst die Kombination aus gehäuften OAuth-Fehlern, verdächtigen Befehlen und einem kurz darauf folgenden TMM-Absturz rechtfertigt eine Untersuchung. Ein fehlender Treffer ist kein Ausschluss, wenn Logs rotiert oder gelöscht wurden.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Gehäufte OAuth-Fehler von einer Quelle, gefolgt von Befehlen im Audit-Log und einem TMM-Absturz auf dem BIG-IP fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare BIG-IP-APM-Virtual-Server mit OAuth-Server-Profil über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre BIG-IP APM-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Heute anordnen: Betroffenheit prüfen und die F5-iRule über den Support anfordern und einsetzen.
- Für jedes BIG-IP mit OAuth-Server-Profil eine forensische Prüfung beauftragen – dokumentiert für eine etwaige Meldung.
- Engineering-Hotfix innerhalb der Woche einspielen und den Umstieg auf den regulären Release einplanen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-94127 und dem BIG-IP APM-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: F5 Security Advisory K000162605 (veröffentlicht 22.09.2026, aktualisiert 23.09.2026) · F5 K000163302 (Engineering-Hotfixes 17.5.1.9 / 17.1.3.5) · CVE-Record CVE-2026-94127 (F5 als CNA) · NVD CVE-2026-94127 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 22.09.2026, Frist 25.09.2026, forensische Triage). Angaben nach bestem Wissen zum Stand 28.09.2026; Hotfix-Stände gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.