AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-53521

Unauthentifizierte Remote-Code-Execution in F5 BIG-IP APM.

Ein nicht authentifizierter Angreifer aus dem Internet kann durch speziell präparierten Datenverkehr an ein BIG-IP-APM-Virtual-Server beliebigen Code ausführen – die vollständige Übernahme des Geräts. Voraussetzung ist eine an einem Virtual Server aktivierte Access Policy. F5 hat die zunächst als DoS eingestufte Lücke im März 2026 zur kritischen RCE hochgestuft; sie wird aktiv zum Ablegen von Web-Shells ausgenutzt.

> **Geschäftsrisiko:** vollständige Kompromittierung eines exponierten Sicherheits-Gateways – mit Potenzial für Datenabfluss, dauerhaften Persistenz-Zugang, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

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 Zutun – vollständiger Verlust von Vertraulichkeit, Integrität und Verfügbarkeit des Systems. Im März 2026 von einer DoS-Lücke (4.0: 8,7 / 3.1: 7,5) zur RCE hochgestuft (4.0: 9,3 / 3.1: 9,8).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2026	BIG-IP APM 15.1 / 16.1 / 17.1 / 17.5 mit Access Policy am Virtual Server	Sofort

Das Wichtigste in 60 Sekunden.

9,3 · KRITISCH
CVSS 4.0 Basiswert

Unauth. RCE
BIG-IP APM Virtual Server

Aktiv
ausgenutzt · CISA KEV · Web-Shells

Kein PoC
öffentlich – aber aktive Ausnutzung

Die Ursache: Der APM-Bestandteil verarbeitet präparierten Datenverkehr fehlerhaft, sobald eine Access Policy an einem Virtual Server hängt. Ein stack-basierter Pufferüberlauf (CWE-121) erlaubt einem nicht authentifizierten Angreifer aus der Ferne die Ausführung beliebigen Codes. Betroffen ist ausschließlich die Datenebene (Data Plane) – ohne dass eine Anmeldung an der Verwaltungsoberfläche nötig wäre.

ANGRIFFSKETTE

01 **APM exponiert** – ein Virtual Server mit Access Policy ist aus dem Internet erreichbar

02 **Crafted Traffic** – speziell präparierte Anfragen an den APM-Dienst

03 **Buffer Overflow** – stack-basierter Überlauf führt zur Code-Ausführung

04 **Web-Shell** – unauth. RCE, teils rein im Speicher, SELinux wird deaktiviert

Betroffenheit & Fixversionen

BIG-IP-Zweig	Verwundbar bis	Fixversion (Ziel)
15.1	< 15.1.10.8	15.1.10.8
16.1	< 16.1.6.1	16.1.6.1
17.1	< 17.1.3	17.1.3
17.5	< 17.5.1.3	17.5.1.3

Angreifbar nur, wenn eine APM-Access-Policy an einem Virtual Server aktiv ist. Ältere, teils abgekündigte Zweige (< 15.1) sowie die exakten Build-Ranges gegen das Hersteller-Advisory K000156741 des eigenen Zweigs abgleichen – dort verbindlich.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder eine RCE kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

15.10.2025
F5 veröffentlicht die Lücke (Quarterly Security Notification) – zunächst als DoS

27.03.2026
CISA nimmt CVE-2025-53521 in den KEV-Katalog auf (Frist Bundesbehörden: 30.03.2026)

28.03.2026
F5 stuft neu ein: DoS → RCE · CVSS 9,8 (3.1) / 9,3 (4.0)

Seither
Aktive Ausnutzung – Web-Shells, teils rein im Speicher; SELinux deaktiviert

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition prüfen, patchen, dann Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Exposition prüfen & einschränken	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob eine APM-Access-Policy an einem Virtual Server hängt und ob dieser aus dem Internet erreichbar ist. BIG-IP-Version gegen die Fix-Tabelle des eigenen Zweigs abgleichen. Nur diese Kombination ist angreifbar.

02 Exposition reduzieren (Zwischenmaßnahme)

F5 nennt **keinen offiziellen Workaround** – nur der Patch schließt die Lücke. Bis zum Einspielen den Zugriff auf betroffene APM-Virtual-Server so weit wie möglich einschränken (Quell-IP-Filter, vorgelagerte Firewall, Zugang nur über VPN).

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`15.1.10.8` · `16.1.6.1` · `17.1.3` · `17.5.1.3`). Dies ist die einzige belastbare Behebung.

04 Kompromittierung ausschließen

Die IoCs unten abgleichen: unerwartete Dateien unter `/run/`, veränderte System-Binaries, bash-Ausführung über das Konto `f5hubblelcdadmin` und das Deaktivieren von SELinux. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff. Bei Verdacht Gerät als potenziell kompromittiert behandeln.

05 Integrität verifizieren

Web-Shells wurden teils rein im Speicher beobachtet – sie hinterlassen ggf. keine Dateispuren. `sys-eicheck`-Integritätsergebnisse sowie modifizierte Binaries (`/usr/bin/umount`, `/usr/sbin/httpd`) auswerten und herstellerseitige Hinweise befolgen.

Kompromittierungs-Indikatoren (IoCs)

LOG-MARKER (RESTJAVAD-AUDIT)

POST `http://localhost:8100/mgmt/tm/util/bash` durch Konto `local/f5hubblelcdadmin` (HTTP 200)

DATEI-MARKER

neu: `/run/bigtlog.pipe`, `/run/bigstart.ltm`
verändert: `/usr/bin/umount`, `/usr/sbin/httpd` (sys-eicheck-Fehler)

SYSTEM-MARKER (AUDITD)

`avc: received setenforce notice (enforcing=0)` – SELinux deaktiviert; Web-Shells teils rein im Speicher

Zur Einordnung: Die aufgeführten IoCs stammen aus den F5- und Analysten-Berichten zur beobachteten Kampagne und sind eine Momentaufnahme. Da Web-Shells rein im Speicher operieren können, ist der Dateisystem-Befund allein kein Ausschluss – die Auswertung der Audit- und Integritäts-Logs ist maßgeblich.

Wichtig: Web-Shells wurden teils ausschließlich im Arbeitsspeicher beobachtet und hinterlassen dann keine dauerhaften Dateispuren. Ohne Auswertung der Audit-Logs und Integritätsprüfungen bleibt ein bereits erfolgter Zugriff unter Umständen unsichtbar.

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: Die bash-Ausführung über das Konto f5hubblelcdadmin und das Deaktivieren von SELinux fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden internet-exponierte, ungepatchte BIG-IP APM Virtual Server mit Access Policy 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-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

- Patch innerhalb von 72 Stunden anordnen; bis dahin die Exposition betroffener APM-Server einschränken.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters und der BIG-IP-Integrität entscheiden.

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-2025-53521 und dem BIG-IP-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2025-53521 · F5 Security Advisory K000156741 / Quarterly Security Notification K000156572 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 27.03.2026) · Arctic Wolf · Beazley Security · Help Net Security. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.