F5 BIG-IP APM critical flaw CVE-2026-94127 under active exploitation



F5 has confirmed active exploitation of CVE-2026-94127 (CVSS 9.8), a heap-based buffer overflow in BIG-IP APM allowing unauthenticated remote code execution. CERT-EU urges prompt hotfixing and a compromise check.

- CVE-2026-94127 has a CVSS score of 9.8 and is a heap-based buffer overflow enabling unauthenticated remote code execution.
- F5 confirmed exploitation in the wild when it published its advisory on 22 September 2026.
- Affected: BIG-IP APM 17.1.0–17.1.3, 17.5.0–17.5.1 and 21.1.0, when an access policy and an OAuth profile are configured on a virtual server.
- An iRule-based mitigation is available through F5 support if patching cannot be done immediately.
- Key warning sign: repeated OAuth failures, then suspicious commands, then a TMM SIGABRT.

What happened

On 22 September 2026, F5 published an advisory on a critical vulnerability in BIG-IP APM and confirmed that it is being exploited in the wild. CERT-EU has issued its own advisory recommending action as soon as possible.

The flaw, **CVE-2026-94127**, carries a CVSS score of 9.8. It is a heap-based buffer overflow that lets an unauthenticated attacker run code remotely on the affected device.

Who is affected

The issue affects BIG-IP APM versions 17.1.0 to 17.1.3, 17.5.0 to 17.5.1, and 21.1.0, but only where an access policy and an OAuth profile are configured on a virtual server.

Checking for compromise

CERT-EU points to vendor-provided indicators. The combination to treat as a trigger for human review is multiple OAuth authentication failures, followed by suspicious commands, shortly followed by a TMM SIGABRT.

- Look in /var/log/apm for repeated OAuth failures, especially 10 or more from one IP in a short window.
- Check OAuth failure statistics for an unexplained rise in total_failed.
- Review /var/log/audit around those timestamps for suspicious commands.
- Investigate TMM core files. A core file alone is not an indicator, but F5 has observed TMM entering a loop that leads the SOD daemon to send a SIGABRT.

Mitigation

If the hotfix cannot be applied immediately, F5 offers an iRule-based mitigation for the affected virtual server. Customers should contact F5 support to obtain it.

What to do now

1. Identify all BIG-IP APM instances and check whether they run an affected version with an access policy and OAuth profile on a virtual server.
2. Preserve forensic evidence (logs, audit records, TMM core files) before making changes.
3. Apply the relevant F5 hotfix as a priority.
4. If patching is delayed, request the iRule-based mitigation from F5 support.
5. Review /var/log/apm, /var/log/audit and OAuth failure statistics for the vendor's indicators of compromise.
6. If any sign of compromise is found, start the incident response process and notify relevant stakeholders per your internal and regulatory obligations.