CERT-EU

Security Advisory 2026-013

# Critical Vulnerability in F5 BIG-IP APM

*2026-09-22 — v1.0*

**TLP:CLEAR**

*History:*

- *22/09/2026 — v1.0 – Initial publication*

## Summary

On 22 September 2026, F5 published an advisory addressing a critical vulnerability affecting its BIG-IP APM product. The vendor **confirmed active exploitation in the wild** [1].

CERT-EU recommends taking appropriate actions as soon as possible.

## Technical Details

The vulnerability **CVE-2026-94127**, with a CVSS score of 9.8, is a **heap-based buffer overflow vulnerability** and allow **unauthenticated** attacker to achieve **remote code execution** (RCE) on the affected device [1].

## Affected Products

The vulnerability affects the following versions of BIG-IP APM **if** configured with an access policy and an OAuth profile on a virtual server [1]:

- 17.1.0 - 17.1.3
- 17.5.0 - 17.5.1
- 21.1.0

## Recommendations

CERT-EU recommends taking the following actions as soon as possible:

1. Preserve forensic evidence.
2. Apply the relevant hotfix.
3. Check for signs of compromise (see the compromise assessment section). If any sign of compromise is detected, start the incident response process.

### Mitigation

If patching cannot be applied immediately, F5 provides an iRule-based mitigation for the affected virtual server. To obtain it, F5 BIG-IP clients should contact the F5 support [1].

### Compromise Assessment

CERT-EU strongly advises to look for the following indicators of compromise provided by the vendor in its advisory [1]:

At a high level, multiple OAuth authentication failures, followed by suspicious commands, shortly followed by a TMM SIGABRT is the combination that should lead to human review of the system.

1. OAuth authentication failures: check `/var/log/apm` for repeated occurrences of the following, especially 10 or more from a single IP in a short window.

```
<DATE> <HOST> err tmm1\[30975\]: 01990004:3: <PROFILE\_NAME>: Request UserInfo from Source ID
  (null) IP <IP> failed. Error Code (invalid\_token) Error Description (The access token is
  invalid.)
```

2. Increase of OAuth failure statistics. Run the following and look for an unexplained increase in `total_failed`:

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

3. Audit log anomalies: if OAuth failures are observed, review `/var/log/audit` around those timestamps for suspicious commands.
4. TMM core files: Presence of a TMM core file alone is not an indicator, but core files should be investigated. The vendor indicates that they have observed TMM entering a loop, which causes the SOD daemon to send a SIGABRT.

## References

[1] https://my.f5.com/manage/s/article/K000162605?mkt_tok=NjUzLVNNQy03ODMAAAGkaH9ofwJ_SRrYgVTlugDrbGmtsu1nH57-t7CLkyTTdZHlyphUFNtULl3ACEteoRszBciQ_4gjkNsWTnQqQfftwYMNCzWPXxGhUqTJ-emmdyUmrf_dqfI