مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in F5 BIG-IP Access Policy Manager (APM)

Tracking #:432319040

Date:31-05-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in F5 BIG-IP Access Policy Manager (APM) that could allow unauthenticated attackers to cause a denial-of-service (DoS) condition by sending specially crafted traffic to vulnerable systems. Successful exploitation may terminate the apmd process, resulting in temporary traffic disruption while services restart.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE:** CVE-2026-40067
- **Severity:** High **CVSS:** CVSS v3.1: 7.5 | CVSS v4.0: 8.7
- The vulnerability exists in BIG-IP APM when an access policy is configured on a virtual server. Specially crafted traffic may cause the apmd process to terminate unexpectedly due to a buffer handling issue classified under CWE-120 (Buffer Copy without Checking Size of Input). This vulnerability can be exploited remotely without authentication, leading to traffic disruption and service interruption.

Affected Products and Versions
Affected Product: BIG-IP APM

- **21.x Branch**
  - 21.0.0
- **17.x Branch**
  - 17.5.0 – 17.5.1
  - 17.1.0 – 17.1.3
- **16.x Branch**
  - 16.1.0 – 16.1.6

Fixed Versions:

- BIG-IP APM 21.x → Upgrade to **21.0.0.1 or later**
- BIG-IP APM 17.5.x → Upgrade to **17.5.1.4 or later**
- BIG-IP APM 17.1.x → Upgrade to **17.1.3.1 or later**

16.x Branch:

- No vendor fix is currently available. Upgrade to a supported branch with available security fixes.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by F5.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://my.f5.com/manage/s/article/K000161056?utm_source=f5support&utm_medium=RSS