مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial-of-Service Vulnerability in F5 BIG-IP

Tracking #:432318428
Date:20-02-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a denial-of-service (DoS) vulnerability in F5 BIG-IP AFM and DDoS Hybrid Defender, where specially crafted traffic can cause the Traffic Management Microkernel (TMM) to terminate and disrupt network traffic.

TECHNICAL DETAILS:

A denial-of-service (DoS) vulnerability exists in F5 BIG-IP AFM and BIG-IP DDoS Hybrid Defender when the Traffic Management Microkernel (TMM) encounters specially crafted traffic. Remote, unauthenticated attackers can exploit this issue to crash TMM, causing temporary disruption of network traffic.

Vulnerability Details

- **CVE-2026-2507**
- **CVSS v4.0:** 8.7 (High)
- **Vulnerability Type:** NULL Pointer Dereference (CWE-476)
- When BIG-IP AFM or BIG-IP DDoS Hybrid Defender is provisioned, crafted traffic can trigger a TMM crash. The TMM process will automatically restart, temporarily disrupting network traffic.

Affected Products

- BIG-IP AFM and DDoS Hybrid Defender 17.5.1.4

Fixed Versions

- Hotfix-BIGIP-17.5.1.4.0.17.20-ENG.iso

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/K000160003