مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Apache HTTP server vulnerabilities in F5 Traffix SDC

Tracking #:432318099

Date:05-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that two recently disclosed Apache HTTP Server vulnerabilities have been identified as affecting F5 Traffix SDC products.

TECHNICAL DETAILS:

Apache has disclosed two vulnerabilities affecting HTTP Server versions up to 2.4.63, involving log injection (CVE-2024-47252) and TLS upgrade-based HTTP desynchronization (CVE-2025-49812). Apache HTTP Server 2.4.64 resolves both issues, with TLS upgrade functionality fully removed.

Vulnerability Details

1. **CVE-2024-47252 – Log Injection in mod_ssl**
   - **Affected:** Apache HTTP Server ≤ 2.4.63
   - **Issue:** Improper escaping of user-controlled SSL/TLS variables during logging, enabling insertion of malicious characters into log files.

2. **CVE-2025-49812 – TLS Upgrade Session Hijacking**
   - **Affected:** Apache HTTP Server ≤ 2.4.63 using SSLEngine optional
   - **Issue:** HTTP desynchronization vulnerability allowing MITM attackers to hijack HTTP sessions during TLS upgrade.

   - **Affected Products:** Traffix SDC 5.2.0
   - **Fix:** Apache 2.4.64

RECOMMENDATIONS:

- Upgrade immediately Apache HTTP Server to fixed version.

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/K000158042