مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

libxslt Vulnerabilities in F5 Traffix SDC

Tracking #:432317596

Date:12-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that F5 has addressed two vulnerabilities in the third-party libxslt library affecting F5 Traffix SDC, which could allow an attacker to execute arbitrary code on affected systems.

TECHNICAL DETAILS:

Two use-after-free vulnerabilities have been identified in the **libxslt** library prior to version **1.1.43**. These flaws can be exploited to execute arbitrary code, potentially leading to system compromise, service disruption, or unauthorized actions.

Vulnerability Details:

- **CVE-2025-24855** – Located in numbers.c, this flaw occurs because, in nested XPath evaluations, an XPath context node can be modified but never restored. It affects xsltNumberFormatGetValue, xsltEvalXPathPredicate, xsltEvalXPathStringNs, and xsltComputeSortResultInternal.
- **CVE-2024-55549** – Located in xsltGetInheritedNsList, this flaw is triggered during exclusion of result prefixes, leading to a use-after-free condition.

Impact

An attacker could leverage these vulnerabilities to execute arbitrary code within the context of the affected application, potentially resulting in:

- Unauthorized system control
- Data corruption or leakage
- Service interruptions

Affected F5 Products:

Product	Branch	Affected Version	Fixed Version	Severity / CVSS v3.1	Vulnerable Component
Traffix SDC	5.x	5.2.0	5.2.0 CF8	High / 7.8	libxslt

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates released by the 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/K000152944?utm_source=f5support&utm_medium=RSS