مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in F5 products

Tracking #:432316384

Date:10-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in F5 products that could be exploited to cause denial-of-service (DoS) conditions on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-25062- libxml2 vulnerability**
- A use-after-free vulnerability exists in libxml2 versions prior to 2.11.7 and 2.12.x before 2.12.5. This vulnerability arises when using the XML Reader interface with DTD validation and XInclude expansion enabled, allowing an attacker to exploit a use-after-free condition during the processing of specially crafted XML documents. This can lead to denial-of-service (DoS) conditions on affected BIG-IP products.
- The vulnerability allows a remote attacker (authenticated in most cases; unauthenticated for BIG-IP Next SPK and CNF) to exploit the use-after-free condition leading to potential crashes or DoS attacks on the affected systems.

Product	Branch	Versions Known to be Vulnerable	Severity/ CVSS	Vulnerable Component or Feature
BIG-IP Next SPK	1.x	1.7.0 - 1.9.2	High/7.5	f5-l4p-engine, f5-debug-sidecar, crd-conversion, mbip-img-waf-policy-converter, policy-builder, f5-downloader
BIG-IP Next CNF	1.x	1.1.0 - 1.3.1	High/7.5	f5-l4p-engine, f5-debug-sidecar, crd-conversion, mbip-img-waf-policy-converter, policy-builder, f5-downloader
BIG-IP (all modules)	17.x	17.1.0 - 17.1.1	Medium/5.3	XML content-based routing, wap monitor, external monitor, AAM image optimization, ASM XML profiles
	16.x	16.1.0 - 16.1.5		
	15.x	15.1.0 - 15.1.10		
Traffix SDC	5.x	5.2.0	High/7.5	libxml2

RECOMMENDATIONS:

- **Limit XML File Sources**: Accept XML files only from trusted users.
- **Monitor for Updates**: Regularly check for updates from F5 regarding patches or fixes for affected products.

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/K000141357?utm_source=f5support&utm_medium=RSS