مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in NGINX JavaScript Module

Tracking #:432319000

Date:20-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in NGINX JavaScript (njs) module allows an unauthenticated remote attacker to trigger a heap-based buffer overflow via improper handling of client-controlled variables in js_fetch_proxy, potentially resulting in denial of service or remote code execution.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-8711**
- **Severity:** Critical **CVSS:** 9.2
- The issue occurs when js_fetch_proxy uses client-controlled variables (e.g., $http_*, $arg_*, $cookie_*) to construct proxy URLs. These values are passed into ngx.fetch(), allowing crafted HTTP requests to corrupt memory in the NGINX worker process, leading to crashes or potential code execution under specific conditions.

Affected Versions

- **NGINX JavaScript (njs):** versions 0.9.4 – 0.9.8

Fixed Versions

- **NGINX JavaScript (njs):** 0.9.9 or later

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/K000161307?utm_source=f5support&utm_medium=RSS