مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in NGINX

Tracking #:432319019

Date:24-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical heap-based buffer overflow vulnerability has been identified in the ngx_http_rewrite_module component of NGINX and affected F5 products.

TECHNICAL DETAILS:

A critical heap-based buffer overflow vulnerability has been identified in the ngx_http_rewrite_module component of NGINX and affected F5 products. The flaw, tracked as CVE-2026-9256, occurs when vulnerable rewrite directives use overlapping unnamed PCRE capture groups together with replacement references inside redirect or argument processing contexts.

Vulnerability Details

- CVE ID: CVE-2026-9256
- CVSS v4.0 Score: 9.2 (Critical)
- Vulnerability Name: NGINX ngx_http_rewrite_module Heap Buffer Overflow
- Vendor: F5 / NGINX
- Affected Component: ngx_http_rewrite_module
- Vulnerability Type: Heap-based Buffer Overflow
- CWE Classification: CWE-122
- Attack Vector: Remote
- Authentication Required: No
- User Interaction Required: None
- Privileges Required: None
- Impact Scope: Data plane only (no control plane exposure)
- Root Cause: Improper handling of overlapping unnamed PCRE capture groups in rewrite directives
- Affected Functionality: Rewrite rules using regex captures such as $1, $2 in redirects or argument processing
- Exploitation Method: Crafted HTTP requests targeting vulnerable rewrite configurations
- Primary Impact:
  - Denial-of-Service (DoS) via worker process crash/restart
  - Possible Remote Code Execution (RCE) under favorable memory conditions
- Exploitation Conditions:
  - Vulnerable rewrite directives configured
  - Overlapping unnamed regex capture groups used
  - ASLR disabled or bypassable for potential RCE
- Recommended Mitigation: Replace unnamed captures with named captures
- Fixed Versions:
  - NGINX Open Source: 1.31.1, 1.30.2
  - NGINX Plus: 37.0.1.1, R36 P5, R32 P7

RECOMMENDATIONS:

- Patch Immediately: Upgrade to the fixed versions listed above.
- Inventory: Identify all NGINX instances (Open Source, Plus, and derivative products) and review their configuration files for vulnerable rewrite directives.
- Refer to F5 Security Advisory K000161377 for detailed version-specific guidance.

- Apply recommended hotfixes or upgrades as per the official tables.

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/K000161377