



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Critical Actively Exploited Vulnerability in NGINX**  
Tracking #:432318986  
Date:18-05-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability affecting both NGINX Open Source and NGINX Plus is being actively exploited in the wild.

## TECHNICAL DETAILS:

A critical security vulnerability affecting both NGINX Open Source and NGINX Plus is being actively exploited in the wild. The flaw, tracked as CVE-2026-42945, is a heap buffer overflow vulnerability within the ngx\_http\_rewrite\_module that may allow unauthenticated attackers to crash NGINX worker processes or potentially achieve remote code execution (RCE) under specific conditions. Security researchers observed exploitation attempts shortly after public disclosure, indicating rapid threat actor weaponization. Organizations are strongly advised to prioritize remediation and configuration reviews immediately.

### Vulnerability Details

- **CVE ID:** CVE-2026-42945
- **Severity:** **Critical**
- **CVSS Score:** 9.2
- **Affected Products:** NGINX Open Source and NGINX Plus
- **Affected Versions:** 0.6.27 through 1.30.0 ,NGINX Plus R32 – R36
- **Fixed Versions:**
  - NGINX Open Source 1.31.0, 1.30.1
  - NGINX Plus R36 P4, R35 P2, R32 P6
- **Vulnerability Type:** Heap Buffer Overflow
- **Affected Component:** ngx\_http\_rewrite\_module
- **Attack Vector:** Remote / Unauthenticated HTTP requests
- **Exploitation Status:** Actively exploited in the wild

## RECOMMENDATIONS:

- **Immediate Actions:** Apply the latest security updates and patches provided by F5 NGINX.

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://nvd.nist.gov/vuln/detail/CVE-2026-42945>