مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in F5 NGINX

Tracking #:432318687

Date:30-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that F5 has disclosed multiple high-severity vulnerabilities affecting NGINX Plus and NGINX Open Source. These vulnerabilities could allow unauthenticated attackers to cause denial-of-service (DoS), crash worker processes, or potentially execute arbitrary code.

TECHNICAL DETAILS:

Vulnerability Details
High-Severity Vulnerabilities
CVE-2026-27654

- A buffer overflow vulnerability in the ngx_http_dav_module may allow an attacker to crash the NGINX worker process or manipulate file paths outside the document root. This issue can be triggered when using MOVE or COPY methods in combination with alias directives.

CVE-2026-27784

- A buffer over-read/overwrite vulnerability in the ngx_http_mp4_module affects 32-bit NGINX Open Source systems. A specially crafted MP4 file can trigger memory corruption, leading to denial-of-service conditions.

CVE-2026-32647

- A vulnerability in the MP4 module affecting both NGINX Plus and Open Source may allow attackers to perform buffer over-read or overwrite operations, potentially causing worker process termination or enabling arbitrary code execution.

CVE-2026-27651

- A flaw in the ngx_mail_auth_http_module can allow unauthenticated attackers to repeatedly crash worker processes when CRAM-MD5 or APOP authentication is enabled, resulting in denial-of-service.

Affected Products

- NGINX Plus: R32 – R36
- NGINX Open Source: 1.0.0 – 1.29.6
- NGINX Open Source (legacy versions): 0.5.13 – 0.9.7

Fixed Versions

- NGINX Plus: R36 P3, R35 P2, R32 P5 or later
- NGINX Open Source: 1.29.7 or later
- NGINX Open Source (legacy branch): 1.28.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/K000160336