مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in NGINX

Tracking #:432319302

Date:16-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed F5 has released security updates to address three memory safety vulnerabilities affecting NGINX Open Source and NGINX Plus.

TECHNICAL DETAILS:

F5 has released security updates to address three memory safety vulnerabilities affecting NGINX Open Source and NGINX Plus, including a critical heap buffer overflow vulnerability (CVE-2026-42533) that may allow remote code execution (RCE) under specific conditions. The vulnerabilities impact components responsible for HTTP request processing, including the map directive, slice module, and SSI module.

Vulnerability Details:

- CVE-2026-42533 – Heap Buffer Overflow in NGINX Map Directive
  CVSS v4.0: 9.2 (Critical)
- CVE-2026-60005 – Uninitialized Memory Access in NGINX ngx_http_slice_module
  CVSS v4.0: 8.8 (High)
- CVE-2026-56434 – Use-After-Free in NGINX ngx_http_ssi_module
  CVSS v4.0: 8.3 (High)

Affected Products:

NGINX Open Source

- Version 1.31.2
- Versions 1.30.0 through 1.30.3

NGINX Plus

- Versions 37.0.0.1 through 37.0.2.1
- Releases R33 through R36

Additional Affected Products

- NGINX Instance Manager 2.17.0 – 2.22.1
- F5 WAF for NGINX 5.9.0 – 5.13.3
- NGINX App Protect WAF 4.x and 5.x
- NGINX Gateway Fabric 1.x and 2.x
- Multiple NGINX Ingress Controller releases

Fixed Versions

Product	Secure Version
NGINX Open Source	1.31.3
NGINX Open Source (Stable)	1.30.4
NGINX Plus	37.0.3.1
NGINX Plus	R36 P7
NGINX Gateway Fabric	2.6.7
NGINX Ingress Controller	5.5.3 / 2026-lts-r4

RECOMMENDATIONS:

Immediate Actions:

- Update all affected F5 products to vendor-recommended versions.
- Verify internet-facing NGINX deployments are running supported versions.

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/K000162100
- https://my.f5.com/manage/s/article/K000162097
- https://my.f5.com/manage/s/article/K000162098