CERT-EU: Five critical NGINX flaws allow unauthenticated remote code execution



F5 disclosed five NGINX vulnerabilities, each rated CVSS 8.1, that let an unauthenticated attacker run code as the worker process. No in-the-wild exploitation is reported; CERT-EU advises prompt updates, internet-facing first.

- Five NGINX vulnerabilities (CVE-2026-123007, CVE-2026-123633, CVE-2026-121810, CVE-2026-123634, CVE-2026-113425) each carry a CVSS score of 8.1.
- All can lead to unauthenticated code execution with the privileges of the NGINX worker process.
- Researchers demonstrated CVE-2026-123007; no exploitation in the wild has been reported yet.
- Affected: NGINX Open Source mainline 1.9.5 to 1.31.8, stable 1.30.x, and NGINX Plus including R34, R35, R36 and several 37.x releases.
- Disabling HTTP/2 on exposed listeners mitigates CVE-2026-123007 and CVE-2026-123633 where

> updating is not immediate.

What was disclosed

On 18 November 2026, F5 published an advisory covering five vulnerabilities in NGINX. CERT-EU summarised them in advisory 2026-022. Each is rated CVSS 8.1, and each can let an unauthenticated remote attacker execute code with the privileges of the NGINX worker process.

The flaws depend on configuration. CVE-2026-123007 is an integer overflow in HTTP/2 flow control and needs only HTTP/2 enabled on a listening port. CVE-2026-123633 and CVE-2026-121810 are use-after-free issues involving HTTP/2 and HTTP/3 (QUIC) connections combined with upstream forwarding. CVE-2026-123634 concerns the DNS resolver waiting list, and CVE-2026-113425 concerns mail proxy authentication via auth_http.

Researchers have demonstrated CVE-2026-123007. No exploitation in the wild has been reported so far.

Who is affected

- NGINX Open Source mainline from 1.9.5 to 1.31.8, depending on the vulnerability
- NGINX Open Source stable 1.30.x, including 1.30.6
- NGINX Plus 37.0.0 to 37.0.7.1, 37.1.0 to 37.2.0.1, and R34, R35, R36

Fixed versions are listed in the F5 advisory.

Recommended response

CERT-EU advises updating as soon as possible, starting with internet-facing instances. If that is not immediately possible, removing http2 from listen directives or setting http2 off; mitigates CVE-2026-123007 and CVE-2026-123633 only.

For compromise assessment, watch the error log for worker processes exiting on a signal. This points to exploitation attempts rather than confirmed code execution, so process creation logs should also be checked.

What to do now

1. Inventory all NGINX Open Source and NGINX Plus instances, including those embedded in appliances, and compare versions with the F5 advisory.
2. Apply the fixed versions from the F5 advisory, starting with internet-facing instances.
3. Where patching must wait, disable HTTP/2 on exposed listeners to mitigate CVE-2026-123007 and CVE-2026-123633, and record the exception.
4. Review configurations for HTTP/3, resolver with proxy_pass built from request data, and mail proxy with

auth_http to gauge exposure to the other three flaws.

5. Search NGINX error logs for worker processes exiting on a signal, and check process creation logs on any host showing them.
6. Track the work under your vulnerability management process in line with NCA ECC patching requirements.