CERT-EU

Security Advisory 2026-022

Critical vulnerabilities in Nginx

2026-11-18 — v1.0

TLP:CLEAR

History:

- *18/11/2026 — v1.0 – Initial publication*

Summary

On 18 November 2026, F5 published an advisory addressing five vulnerabilities in NGINX that allow an unauthenticated remote attacker to execute code with the privileges of the NGINX worker process [1, 2].

While researchers managed to successfully demonstrate the use of CVE-2026-123007 [1], no exploitation in the wild has been reported yet.

It is recommended to swiftly update NGINX as soon as possible, prioritising internet facing appliances.

Technical Details

The vulnerability **CVE-2026-123007**, with a CVSS score of 8.1, is an integer overflow in HTTP/2 flow control which causes an out-of-bounds write on the heap. The only precondition is HTTP/2 enabled on a listening port.

The vulnerability **CVE-2026-123633**, with a CVSS score of 8.1, is a use-after-free flaw occurring when connection draining closes an active HTTP/2 connection while NGINX connects to an upstream server. HTTP/2 should be enabled and requests should be forwarded to an upstream server.

The vulnerability **CVE-2026-121810**, with a CVSS score of 8.1, is a use-after-free flaw occurring when a QUIC connection is drained during stream creation and upstream connection. HTTP/3 should be enabled and requests should be forwarded to an upstream server.

The vulnerability **CVE-2026-123634**, with a CVSS score of 8.1, is a use-after-free flaw occurring in the processing of the DNS resolver waiting list. a `resolver` must be set, a `proxy_pass` destination built from request data, and `mirror` with `mirror_request_body off` should be configured.

The vulnerability **CVE-2026-113425**, with a CVSS score of 8.1, is a use-after-free occurring when the client closes the connection during the `auth_http` authentication lookup. A mail proxy must be configured with `proxy on` and `auth_http`.

All five vulnerabilities can lead to unauthenticated code execution with the privileges of the NGINX worker process [1].

Affected Products

The following products and versions are affected by one or more of the above vulnerabilities:

- NGINX Open Source (mainline) from version 1.9.5 to 1.31.8 (range depends on the vulnerability, see Technical Details) [1]. Refer to the vendor advisory for the information on fixed versions [2].
- NGINX Open Source (stable) versions 1.30.x, including the current stable version 1.30.6 [1, 3]. Refer to the vendor advisory for the information on fixed versions [2].
- NGINX Plus from version 37.0.0 to 37.0.7.1, and 37.1.0 to 37.2.0.1. The versions R34, R35 and R36 are also affected [2]. Refer to the vendor advisory for the information on fixed versions [2].

Recommendations

CERT-EU recommends updating vulnerable instance as soon as possible, prioritising internet-facing devices.

Compromise assessment

It is possible to monitor for crashes of the Nginx worker (`worker process ... exited on signal` in the error log). However, this is not a high-fidelity indicator of successful remote code execution but rather an indication of exploitation attempts. Further checks in the process creation logs are necessary.

Mitigation

When updating is not immediately possible, disabling HTTP/2 on exposed listeners (by removing the `http2` from the `listen` directives, or set `http2 off;`) mitigates the vulnerabilities CVE-2026-123007 and CVE-2026-123633 [1].

References

[1] https://xint.io/blog/nginx2root-remote-code-execution

[2] https://my.f5.com/manage/s/article/K000164058

[3] https://nginx.org/en/security_advisories.html