AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

SECURITY ALERT

nginx2root: remote code execution in NGINX through HTTP/2

Contents

I. Background 3
II. Vulnerability details 3
Affected and fixed versions 4
III. Attack vector 5
IV. Exploitation status 5
V. Exposure in Africa and Cameroon 5
VI. Conclusion and recommended actions 6
VII. References 6

I. Background

On 18 November 2026, F5 released out-of-band fixes for five critical vulnerabilities affecting NGINX, the most widely used web server and reverse proxy in the world. The most severe, tracked as CVE-2026-123007 and dubbed "nginx2root", lies in the HTTP/2 module and has existed for more than eleven years: it affects every release since 1.9.5 (September 2015).

F5 gives all five flaws a CVSS v4.0 score of 9.2 (critical). They allow an unauthenticated attacker to execute code on the server with the privileges of the NGINX worker processes. All five were discovered by the Xint (Theori) research team; the main one, CVE-2026-123007, was also reported separately by Wiz Research, Rapid7 and Ikotas Labs. Teams at Wiz, Xint and Rapid7 demonstrated exploitation of that flaw, and Luxembourg's CIRCL published response guidance.

II. Vulnerability details

The main vulnerability, nginx2root, is a memory corruption flaw in HTTP/2 flow control: an integer overflow in the handling of send windows leads to an out-of-bounds read and write on the heap. Four other flaws, all use-after-free vulnerabilities fixed at the same time, affect more specific NGINX configurations. The NGINX project uses its own severity scale, separate from F5's CVSS score: on that scale it rates CVE-2026-123007 and CVE-2026-113425 "major" and the other three "medium".

CVE	Exploitation condition	CVSS v4.0 score
CVE-2026-123007 (nginx2root)	HTTP/2 enabled (versions 1.9.5 to 1.31.8)	9.2 Critical
CVE-2026-123633	HTTP/2 enabled, requests passed to an upstream server while the worker is low on available connections (worker_connections); versions 1.19.7 to 1.31.8	9.2 Critical
CVE-2026-123634	DNS resolver configured and upstream server name built from variables, with an SSI or mirror subrequest; versions 0.6.18 to 1.31.8	9.2 Critical
CVE-2026-121810	HTTP/3 enabled, requests passed to an upstream server; versions 1.25.0 to 1.31.8	9.2 Critical
CVE-2026-113425	NGINX used as a mail proxy with auth_http; versions 0.5.33 to 1.31.8	9.2 Critical

Alias	nginx2root (CVE-2026-123007)
Product	NGINX Open Source and NGINX Plus
Type	Memory corruption (integer overflow) in HTTP/2 flow control
Impact	Unauthenticated remote code execution
CVSS v4.0 score	**9.2 Critical (F5's assessment)**
Exploitation status	**Exploit code published by Rapid7; no real-world attack reported as of 19 November 2026**
Discovered by	Xint (Theori); reported separately by Wiz Research, Rapid7 and Ikotas Labs
Disclosure date	18 November 2026
Fix	NGINX 1.31.9 and 1.30.7, NGINX Plus 37.3.0.1 and 37.0.8.1

Affected and fixed versions

The following versions are affected. At the time of writing (19 November 2026), Ubuntu (16.04 to 26.10), Debian (bookworm, trixie, forky), Red Hat Enterprise Linux, SUSE and Amazon Linux 2 had not yet published a fixed package; fixed packages were available for Alpine 3.24, AlmaLinux and Amazon Linux 2023. Distributions backport fixes without changing the version number: refer to each distribution's security tracker.

Product	Affected versions	Fixed versions
NGINX Open Source (mainline)	1.31.0 to 1.31.8	1.31.9 or later
NGINX Open Source (stable and older branches)	1.9.5 to 1.30.6	1.30.7 or later
NGINX Plus 37.1 to 37.2	37.1.0 to 37.2.0.1	37.3.0.1 or later
NGINX Plus 37.0	37.0.0 to 37.0.7.1	37.0.8.1 or later
NGINX Plus R34 to R36	All	No fix: migrate to a fixed 37.x version
Official Docker images	Prior to the fixes	Tags 1.31.9 and 1.30.7 (including Alpine); pull the latest, mainline and stable tags again and rebuild derived images

III. Attack vector

Exploitation of nginx2root unfolds as follows:

- The attacker opens an HTTP/2 connection to an exposed NGINX server, without any authentication.
- The attacker sends a large volume of specially crafted HTTP/2 frames that corrupt the flow-control window accounting and then the worker process memory.
- The attacker gains code execution with the NGINX worker privileges, allowing traffic interception, theft of certificates and secrets, or lateral movement to upstream servers.
- By chaining this flaw with a separate, still unpatched Linux kernel vulnerability (SCTP module), Xint researchers obtained root privileges on the host, even from inside a Docker container.

The attack requires bypassing ASLR, which Wiz and Xint achieved in their tests. Rapid7's exploit also depends on a glibc memory copy routine specific to x86-64 systems and needs about 128 GB of HTTP/2 traffic over a single connection: its demonstration took 2 minutes 30 seconds, and the attack fails on links that are too slow. Xint's attack worked against test servers hosted on AWS, GCP and Azure over public IP addresses.

IV. Exploitation status

As of 19 November 2026, neither F5, Wiz, Rapid7 nor Xint report any real-world attack, and none of the five flaws is listed in CISA's Known Exploited Vulnerabilities (KEV) catalogue. However, exploit code is public: Rapid7 has published its own on GitHub for CVE-2026-123007, even though in its current form it only works under lab conditions. Xint and Wiz, whose attacks succeeded against real servers, are withholding theirs. Fake repositories posing as exploit code are also circulating and should be avoided.

The release of Rapid7's code and Xint's demonstration of successful attacks against Internet-facing cloud servers make the rapid appearance of more reliable exploits likely. NGINX servers are a prime target because they sit in front of a very large number of services.

V. Exposure in Africa and Cameroon

NGINX is very widely deployed in Cameroon and across Africa as a web server, reverse proxy, load balancer and API gateway. It fronts government portals, banking and mobile money platforms, telecommunications operators' services and many sites hosted locally or in the cloud.

HTTP/2 is enabled in the vast majority of recent HTTPS configurations. In addition, many servers run Linux distribution packages that were not yet fixed at the time of writing, or old

versions that have never been updated, which greatly increases national exposure. No public measurement of the number of vulnerable servers in Cameroon is available to date.

VI. Conclusion and recommended actions

nginx2root is a critical vulnerability that allows remote compromise of NGINX servers without authentication. The CIRT strongly recommends the following actions:

1. Inventory all NGINX servers, including Docker images, Kubernetes Ingress controllers and appliances embedding NGINX, and record their versions.
2. Update without delay to NGINX 1.31.9 or 1.30.7, or NGINX Plus 37.3.0.1 or 37.0.8.1, then fully restart the service: a simple reload does not replace the running binary and leaves old worker processes running. For NGINX packages supplied by Linux distributions, apply the fixed package as soon as it is published and, in the meantime, apply measure 3.
3. Until the update is applied, temporarily disable HTTP/2: from version 1.25.1, add the "http2 off;" directive and remove the http2 parameter from listen directives; on older versions, remove the http2 parameter from listen directives. Then confirm with openssl s_client that the h2 protocol is no longer negotiated. This measure protects only against the two HTTP/2 flaws (CVE-2026-123007 and CVE-2026-123633), not against the other three.
4. Disable HTTP/3 where it is not essential, replace upstream server names built from variables with fixed upstream groups, disable the mirror directive where it is not needed, and restrict the mail proxy to the loopback interface or to trusted networks.
5. Where SCTP is not used, block loading of the corresponding module (add "install sctp /bin/false" to a .conf file in /etc/modprobe.d/), since the kernel flaw is not yet patched. This measure does not unload a module that is already loaded.
6. Monitor for unexpected processes launched by NGINX workers, abnormal exits or core dumps, long-lived HTTP/2 connections with heavy inbound traffic but few logged requests, and unusual outbound connections.
7. Bear in mind that a clean access log does not rule out an attack, and report any suspected incident to the CIRT.

For any incident or request for assistance, contact the CIRT through its usual channels.

VII. References

- NGINX (official project), security advisories: https://nginx.org/en/security_advisories.html
- NGINX, version 1.30.7 changelog: https://nginx.org/en/CHANGES-1.30
- F5, advisory K000163926 on CVE-2026-123007: https://my.f5.com/manage/s/article/K000163926
- F5, out of band security notification of 18 November 2026 (K000164058): https://my.f5.com/manage/s/article/K000164058
- NIST, National Vulnerability Database (NVD): https://nvd.nist.gov/vuln/detail/CVE-2026-123007

- MITRE, CVE Program: https://www.cve.org/CVERecord?id=CVE-2026-123007
- CIRCL, Vulnerability Lookup: https://vulnerability.circl.lu/vuln/CVE-2026-123007
- Red Hat, CVE page: https://access.redhat.com/security/cve/cve-2026-123007
- Ubuntu, security tracker: https://ubuntu.com/security/CVE-2026-123007
- Debian, security tracker: https://security-tracker.debian.org/tracker/CVE-2026-123007
- Xint, nginx2root research report: https://xint.io/blog/nginx2root-remote-code-execution
- Wiz Research, NGINX HTTP/2 RCE vulnerabilities: https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities
- Tenable, nginx2root FAQ: https://www.tenable.com/blog/nginx2root-cve-2026-123007-frequently-asked-questions-about-five-critical-nginx
- Sophos, nginx2root security advisory: https://www.sophos.com/en-us/security-advisories/sophos-sa-20261118-nginx2root
- The Hacker News, 18 November 2026: https://thehackernews.com/2026/11/10-year-old-nginx-http2-flaw-lets.html

