NGINX2Root: five nginx flaws, a Linux kernel bug, and why turning off HTTP/2 is not enough

19 November 2026 · 6 min read · blogs.iictp.org/nginx2root-nginx-http2-rce-sctp-linux-root

The security company Xint published research on 18 November 2026 describing five nginx vulnerabilities that it says can each lead to remote code execution, in different configurations. It also describes a separate Linux kernel flaw that it says can turn code execution as an nginx worker into root on the host. Xint calls the set nginx2root. nginx released fixes the same day.

TL;DR The short version

- Xint published research on 18 November 2026 on five nginx vulnerabilities that can each lead to remote code execution in some configurations.
- It also describes a Linux kernel flaw that can turn code execution as an nginx worker into root on the host.
- Update to nginx 1.31.9 or 1.30.7 and fully restart, because a configuration reload does not replace the binary, and patch the kernel too.

Read online, listen to it, or change the text size: https://blogs.iictp.org/nginx2root-nginx-http2-rce-sctp-linux-root

What was reported

- Xint says the most serious flaw, CVE-2026-123007, lets an unauthenticated attacker run commands on a server with HTTP/2 enabled, with the privileges of the nginx worker process. It describes an integer overflow in HTTP/2 flow control.
- The other four, according to Xint, are use-after-free bugs: CVE-2026-123634 (resolver), CVE-2026-123633 (HTTP/2 with an upstream), CVE-2026-121810 (HTTP/3 with an upstream) and CVE-2026-113425 (mail proxy using auth_http).
- The nginx security advisories list all five as fixed in 1.31.9 and 1.30.7. nginx rates CVE-2026-123007 and CVE-2026-113425 as major and the other three as medium, while Xint describes all five as critical.
- Xint says the kernel flaw is in the SCTP send path, dates from Linux 4.15, and in its tests also gave root on the host from nginx running in a Docker container. LWN reported on 18 November that a kernel patch was not yet available.
- Xint reports that Shodan returned 56.7 million hosts for nginx on 10 November, that 11.94 million showed an identifiable version, and that 98.9% of those fell in the affected range. Xint cautions that these version strings do not confirm a server is vulnerable.

What a practitioner should do

- Update to nginx 1.31.9 or 1.30.7, or to your distribution's fixed package. Xint notes that distributions may backport fixes without changing the version nginx reports, so compare the full package version with the distribution's advisory.
- Restart nginx or complete a supported live binary upgrade. Xint warns that a configuration reload does not replace the running executable.
- If you must wait, match mitigations to your configuration. Xint says disabling HTTP/2 blocks only two of the five flaws. HTTP/3, request-time DNS lookups and the mail proxy each need their own measures, which its report sets out.
- On hosts that do not use SCTP, Xint suggests adding install sctp /bin/false to a .conf file under /etc/modprobe.d/ until a kernel fix is available. It says this does not unload a module already loaded and does not affect SCTP built into the kernel.
- Look beyond the access log. Xint says the HTTP/2 control frames used in the attack are not logged as requests, and suggests watching for programs started by nginx workers, abnormal worker exits, and connections receiving far more data than their logged requests explain.

The wider lesson

A container is not a security boundary against a kernel flaw, and a single mitigation rarely covers a family of bugs. Knowing which protocols and modules each server actually has enabled turns an alert like this into a short checklist. That is the operational discipline the Infrastructure & Security domain of the TPBOK asks of a practitioner.

> Facts in this post were read from the sources listed below on 19 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. Xint. NGINX2Root: New Remote Code Execution Vulnerabilities in nginx Require Urgent Patching. 18 November 2026. xint.io/blog/nginx2root-remote-code-execution
2. nginx. nginx security advisories. Read 19 November 2026. nginx.org/en/security_advisories.html
3. nginx. CHANGES, nginx 1.31.9. 18 November 2026. nginx.org/en/CHANGES
4. LWN.net. NGINX2Root: Remote Code Execution vulnerabilities in nginx. 18 November 2026. lwn.net/Articles/1108362/

Published by IICTP, an independent technical credential body, on 19 November 2026. The current version of this post is at https://blogs.iictp.org/nginx2root-nginx-http2-rce-sctp-linux-root. More guides: blogs.iictp.org.