FOUND BY

NGINX2Root

From nginx visitor to root of the server host

CVE-2026-123007 CVE-2026-123634 CVE-2026-123633 CVE-2026-121810 CVE-2026-113425

How to Fix it Full Writeup

OVERVIEW

What is NGINX2Root?

nginx2root is a collection of five distinct nginx vulnerabilities and one Linux kernel vulnerability. Each has a proven exploit. The most severe enables unauthenticated remote code execution; chained with a separate Linux kernel vulnerability, it can lead to host root.

Severity Critical	Access Remote, no authentication
Affected nginx 1.9.5 – 1.31.8	Fix 1.31.9

Team Xint Research and responsible disclosure · Soomin Shin (imssm99), Joohyun Park (cdor1), Tim Becker (tjbecker), Yves Bieri (yves.bieri)

Five nginx findings and one kernel vulnerability

Each CVE has its own proven exploit. The most severe of the five allows unauthenticated remote code execution on web servers running a common nginx configuration. This remote code execution can be chained with a separate Linux kernel vulnerability to reach host root, remotely and without authentication.

Demonstrated path to root

Specifically, the most severe vulnerability is in nginx HTTP/2 flow control. An unauthenticated remote attacker can corrupt memory in an nginx worker, leak memory addresses, and overwrite the pointer to a cleanup function that runs when a connection closes. This can be used to execute commands with worker privileges and receive the output over an existing connection.

The demonstrated entry point needs an externally reachable HTTP/2 port. From there, the exploit corrupts the send window, leaks memory addresses, and executes commands with nginx worker privileges.

nginx hosts in the affected version range

The HTTP/2 vulnerability has existed since nginx introduced HTTP/2 in 2015. In a November 10, 2026 snapshot, 98.9% of hosts with identifiable nginx versions ran releases within the affected version range. That number describes version prevalence; it does not establish whether each host exposes HTTP/2 or has received a backported fix.

Version prevalence, not a count of exploitable endpoints. Source: Shodan

nginx share of websites

Attackers can fingerprint nginx with widely available tools and identify exposed deployments. W3Techs estimates that nginx is used by about 30% of websites whose web server it can identify.

about 30%

nginx Other web servers

Source: W3Techs

How Xint found NGINX2Root

nginx runs roughly a third of the web and has been fuzzed and audited by the best researchers in the world for two decades. Pre-auth RCE in nginx almost never happens. The best known one is from 2013. This year every AI lab pointed models at it. Everyone figured the easy bugs were long gone. While testing a new Xint capability ahead of ZeroDay Cloud, a Xint researcher pointed it at a slice of nginx, about 50,000 lines. He picked the target; Xint did the rest. Ninety minutes later it flagged high severity issues with reproduction steps specific enough to become a working exploit in under ten minutes.

The human researcher was the one that found the specific vuln that affects a default nginx setup with HTTP/2 enabled. This discovery was around the same time this same researcher found another critical vulnerability in a different project that we cannot talk about yet due to the same concerns as nginx2root. We took those learnings and incorporated them into the harness as a new, general Xint feature (that is, not fine-tuned to nginx), which then found the other 4 critical nginx vulnerabilities with no human guidance. All five were found independently; one was also found by other researchers around the same time.

IMPACT

Why our findings matter

The impact depends on how widely the affected code is deployed and whether the attack works in realistic environments. We examined nginx version prevalence and validated the attack chain in controlled cloud environments.

The HTTP/2 code path dates to nginx 1.9.5 in 2015. In Xint's November 10, 2026 Shodan snapshot, 11.8 million of 11.94 million version-identifiable nginx hosts ran releases in the affected range. That is a measure of version prevalence, not a count of exploitable endpoints. Xint also found that 88.6% of Fortune 500 companies use nginx.

Xint surfaced the initial flaw without human guidance, and its researchers followed it beyond a crash. The team validated the chain in controlled AWS, GCP, and Azure setups, including public HTTPS paths.

EXPOSURE

Who is affected?

The version range below applies to the HTTP/2 remote-code-execution finding, the most severe of the five. Official nginx releases from 1.9.5 through 1.31.8 contain the affected code. Exposure requires HTTP/2 support in the nginx build and an affected listener that accepts HTTP/2 connections.

Each of the other four CVEs is a distinct vulnerability with its own affected range and exploit. Check its individual advisory rather than applying the HTTP/2 finding's version range to all five.

Distribution packages, appliances, and container images may backport a security fix while retaining an older version string. Confirm patch status from the relevant vendor advisory instead of relying on `nginx -v` alone. The host-root stage uses a separate Linux SCTP kernel vulnerability and must be assessed separately.

Quick check for the HTTP/2 finding

All five conditions must hold for a host to be exposed

REMEDIATION

How do I fix it?

Apply the fixed nginx release or your vendor's security update as soon as it is available. If you cannot update immediately, disable HTTP/2 on every affected nginx listener until the fix is applied. This mitigates the HTTP/2 finding; follow the separate advisories for the other four CVEs and the Linux kernel finding.

DEMO

See it in action

AWS GCP Azure Bare Metal

TECHNICAL DETAILS

Five findings. Five exploits. One demonstrated path to root.

The sequence below describes the most severe HTTP/2 finding. The other four CVEs are distinct vulnerabilities with separate exploit analyses.

Disclosure timeline

39 days from discovery to fix (KST)

☐ **2026 Oct 11**
Found

☐ **2026 Oct 16**
Reported to F5 via HackerOne

☐ **2026 Nov 19**
Fix released

References

Xint Blog
Further technical details are available on the Xint blog.

nginx release
The nginx fix is documented in the official announcement.

FAQ

Frequently asked questions

About nginx2root

5 questions

What is nginx2root?

nginx2root refers to five nginx vulnerabilities and a separate Linux kernel SCTP vulnerability discovered by Theori’s Xint research team. The nginx vulnerabilities affect a variety of configurations, and the Xint team demonstrated remote code execution using each vulnerability independently. Each nginx vulnerability can be chained with the Linux kernel vulnerability to obtain root privileges on the host.

What privileges can an attacker gain?

How serious is it?

Is it being exploited?

Will the exploit be published?

Checking exposure

8 questions

Which nginx configurations should I check?

How do I check whether I am affected by CVE-2026-123007?

Can an older version number still indicate a patched package?

Am I safe if I disable HTTP/2?

What if nginx is only accessible from an internal network?

What changes if I run nginx in Docker or Kubernetes?

Does a CDN or load balancer protect my nginx server?

How do I check products that include nginx?

Updates and mitigations

5 questions

What should I do first?

Which release or package should I install?

Is reloading the configuration enough after updating nginx?

Will disabling HTTP/2 affect my application?

Can a web application firewall or connection limits replace patching?

Investigating a possible compromise

3 questions

What should I investigate?

Can ordinary access logs establish that no attack occurred?

What should I do if I confirm a compromise?

The kernel bug

1 question

Does patching nginx close the whole chain?

Disclosure

3 questions

When was it reported and fixed?

Who found it?

Where can I find updates?

01 What is NGINX2Root?

The platform behind the discovery

Contact Xint

Xint is an AI pentesting platform that analyzes source code and tests live applications the way an attacker would, then surfaces the vulnerabilities that are actually exploitable. It's the platform that found CopyFail (`CVE-2026-31431`) in Linux, and now in nginx.

- World-record 9x DEF CON CTF Champions
- 2026 Cybersecurity Awards: Best Autonomous Pentesting Platform
- Part of Anthropic's Cyber Verification Program and OpenAI's Daybreak

Protecting software used by billions

Google
Microsoft
OpenAI
SAMSUNG
okta
DARPA
and more

First Name*
Last Name*
Job Title*
Company Name*
Work Email Address*
Country/Region*

Tell us more about your request.*

Providing details such as your expected timeline, project scope, or budget range will help us respond more quickly and accurately

By submitting this form, you acknowledge that we will process your data for marketing purposes in accordance with our Privacy Policy. You can object to receiving direct marketing at any time via the unsubscribe links in our emails.

Submit

Team behind NGINX2Root

Xint Research Team

Soomin Shin
Xint Researcher

Joohyun Park
Xint Researcher

Tim Becker
Xint Researcher

Yves Bieri
Xint Researcher

Hyuk Kwon
Head of Cyber Research

Juno Im
Head of AI & Cyber Research Group

Brian Pak
Chief Executive Officer

FOUND BY Xint

© 2026 Theori. All Rights Reserved.