nginx2root exploit chain

campaign · nginx2root first reported 18 Nov 2026 10 sources

v9 · updated 23 Nov 2026, 16:27 UTC

also reported as CVE-2026-123007 · CVE-2026-123633 · Drainbreak · NGINX2Shell

> UNCLEAR — "ACTIVE" IS NOT SHOWN BY A QUOTE

BOTTOM LINE

Five critical unauthenticated NGINX RCEs (NGINX2Root/NGINX2Shell) allow command execution as the nginx worker; an unpatched Linux SCTP kernel bug can be chained to reach host root; patches and HTTP/2 disablement mitigate the worst exposure. Public PoCs exist; no confirmed mass exploitation yet.[1,2,5]

FOR THE BOARD

Multiple critical unauthenticated NGINX RCEs were disclosed and patched; patch internet-facing NGINX, disable HTTP/2 if needed, and confirm kernel fixes to prevent full host compromise.

ARE YOU EXPOSED?

TARGETS Internet-facing NGINX with HTTP/2 enabled; various nginx modules and Linux kernels.[2,3,8]

Check internet-facing NGINX versions/configs, HTTP/2 enabled, resolver/mail/proxy usage, and kernel SCTP module.

WHAT TO DO

1. **If you cannot patch immediately, disable HTTP/2 on affected listeners.**[3,7]
   CVE-2026-123007 and CVE-2026-123633 require HTTP/2; disabling reduces exposure to the most severe bugs.
2. **Verify Linux kernel/SCTP fixes before trusting containment.**[1,8]
   Xint found an unpatched SCTP kernel use-after-free that can be chained to escalate from worker to root; distributions pending fixes.
3. **Hunt for unexpected NGINX worker crashes, spawned processes, and anomalous HTTP/2 traffic.**[1,6]
   Exploitation can crash workers, leak heap addresses, execute commands, and PoCs transmit large HTTP/2 frames.

Timeline

November 18, 2026	DISCLOSURE	Coordinated disclosure and out-of-band security updates for multiple NGINX vulnerabilities [1] *“Nginx, the web server estimated to power a third of the internet, has shipped fixes for multiple vulnerabilities, including a critical unauthenticated remote code execution flaw that puts millions of websites at risk and has existed in the code for over a decade.”*
November 18, 2026	DISCLOSURE	Rapid7 published technical analysis and public PoC for CVE-2026-123007 [2] *“Rapid7 published a technical analysis of CVE-2026-123007 on November 18, and its author, Stephen Fewer, released a public PoC on GitHub at sfewer-r7/CVE-2026-123007.”*
November 18, 2026	PATCH	F5 released out-of-band patches for NGINX including fixes for NGINX2Root [5] *“F5 on Wednesday announced patches for 22 vulnerabilities, including five critical-severity NGINX bugs that could lead to unauthenticated remote code execution (RCE).”*

What they did

Public PoC published for CVE-2026-123007 and multiple teams built exploits/demos. [2]

“Rapid7 published a technical analysis of CVE-2026-123007 on November 18, and its author, Stephen Fewer, released a public PoC on GitHub at sfewer-r7/CVE-2026-123007.”

Whom they target

Targets are not described.

Malware and tools

Public PoC exploit for CVE-2026-123007 (Rapid7 GitHub) [2]

“Rapid7 published a technical analysis of CVE-2026-123007 on November 18, and its author, Stephen Fewer, released a public PoC on GitHub at sfewer-r7/CVE-2026-123007.”

Xint demo videos and internal PoCs; other teams' PoCs/demos [1]

“Xint alled CVE-2026-123007 highly exploitable, saying an externally reachable TLS/HTTP/2 port was enough to corrupt the send window, disclose addresses, and execute commands, and validated the attack over public IPs on AWS, GCP, and Azure under concurrent traffic.”

Attribution

No attribution is given.

Disruption, advisories and law enforcement

None reported.

ATT&CK techniques

The sources do not describe the attacker's behaviour closely enough to map.

Indicators

None published in the sources.

Not known yet

- Exact exploitation count in the wild
- Full technical details of the SCTP kernel bug (withheld)
- Which distributions already backported fixes

Sources

1 **CSO Online** · 18 Nov 2026 · AI unearths ‘internet breaker’ flaws in Nginx web server · archived copy

2 **Tenable blog** · 19 Nov 2026 · NGINX2Root FAQ: Five vulnerabilities in NGINX (CVE-2026-123007) | Tenable® · archived copy

3 **GBHackers** · 19 Nov 2026 · NGINX2Root: Five Critical Vulnerabilities Allow Unauthenticated Attackers to Execute Commands on NGINX Servers · archived copy

4 **Security Affairs** · 19 Nov 2026 · nginx2root:AI Discovers Five Critical nginx Flaws and a Path to Root · archived copy

5 **SecurityWeek** · 19 Nov 2026 · F5 Patches Critical NGINX2Root Flaws as PoC Exploits Go Public · archived copy

6 **Help Net Security** · 19 Nov 2026 · NGINX2Root: F5 patches five critical NGINX vulnerabilities - Help Net Security · archived copy

7 **CrowdStrike blog** · 19 Nov 2026 · CrowdStrike Helps Identify, Patch, and Protect Against NGINX2Root (CVE-2026-123007 et al.) · archived copy

8 **Cloudflare blog** · 20 Nov 2026 · nginx2root: five new nginx vulnerabilities, and how Cloudflare protects origins from the worst of them · archived copy

9 **Security Affairs** · 22 Nov 2026 · Security Affairs newsletter Round 605 by Pierluigi Paganini – INTERNATIONAL EDITION · archived copy

10 **The Hacker News** · 23 Nov 2026 · ⚡ Weekly Recap: VMware 0-Day, Java4Shell, NGINX2Root, Ruby2Shell, and a Whole Lot of Shell Trouble · archived copy

ABOUT THIS REPORT

Compiled by Transilience Newsroom from 10 public sources. Every quotation is checked against the article it cites; 13 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 9, written 23 Nov 2026, 16:27 UTC (threat-report-2026-09-25b).