PatchMon PATCHMON BLOG

NGINX2Root (CVE-2026-123007): Patch Your nginx Fleet

NGINX2Root is fixed in nginx 1.31.9 and 1.30.7. What Ubuntu, Debian, RHEL, Alpine and Amazon Linux shipped, and how to prove every server is patched.

AUTHOR

PatchMon Team

PUBLISHED

19 November 2026

CATEGORIES

Security, Patch Management

READ ONLINE

https://patchmon.net/blog/nginx2root-cve-2026-123007-nginx-rce-patch

Contents

1. The Short Version
2. What NGINX2Root Actually Is
   - Where "2Root" comes from
4. Why This One Hurts More Than the Usual nginx CVE
5. Exploitation So Far
6. Which nginx Versions Are Fixed
7. What Your Distro Is Shipping
   - Ubuntu
   - Debian
   - RHEL, Rocky Linux and AlmaLinux
   - Amazon Linux
   - Alpine and containers
   - Kubernetes ingress-nginx and OpenResty
14. If You Cannot Patch Right Now
15. How to Tell Your Fleet Is Actually Patched
16. Frequently Asked Questions
17. Bottom Line
18. Sources and Further Reading

> ***Last updated: 19 November 2026.*** *Distro status in this post was checked against each vendor's own tracker at 07:20 UTC on 19 November 2026. Debian, Red Hat and SUSE have not shipped fixes yet, so we will keep the tables below current as they do.*

If you run a Linux server that talks to the internet, there is a good chance nginx is on it. It might be the web server, the reverse proxy in front of an app, the ingress controller in a Kubernetes cluster, or the thing a vendor appliance quietly bundled.

On 18 November 2026 the nginx project released **nginx 1.31.9 and 1.30.7**, fixing ten vulnerabilities. Five of them, led by **CVE-2026-123007**, are what researchers at Xint have named **NGINX2Root**: memory corruption bugs that an unauthenticated attacker can reach over the network, each of which Xint says leads to remote code execution. Xint then chained them with a separate, still unpatched Linux kernel bug to get root on the host, including from inside a Docker container.

The fix is out. The question for most teams is how many of their nginx processes are still running the old code.

The Short Version

If you only have two minutes:

What it is: Five memory corruption bugs in nginx: HTTP/2 flow control (CVE-2026-123007 (https://www.cve.org/CVERecord?id=CVE-2026-123007)), HTTP/2 connection handling (CVE-2026-123633), the resolver (CVE-2026-123634), HTTP/3 (CVE-2026-121810) and the mail proxy (CVE-2026-113425).

Severity: F5, the CVE numbering authority for nginx, scores all five **CVSS v4.0 9.2** (CVSS v3.1 8.1). nginx's own advisory rates CVE-2026-123007 and CVE-2026-113425 "major" and the other three "medium".

Who is affected: Any nginx from 1.9.5 to 1.31.8 with HTTP/2 enabled is exposed to the lead bug. The others need specific features: HTTP/2 proxying, request-time DNS with subrequests, HTTP/3, or the mail proxy.

Fixed in: nginx 1.31.9 (mainline) and 1.30.7 (stable). NGINX Plus 37.0.8.1 and 37.3.0.1.

Exploitation so far: No reported exploitation in the wild, and none of the five is in CISA's KEV catalogue as of 19 November. A public proof of concept exists but only works in lab conditions.

What you do about it: Install your distro's or nginx.org's fixed package, then **restart nginx**. A reload does not replace the running binary.

What NGINX2Root Actually Is

Xint's technical write-up (https://xint.io/blog/nginx2root-remote-code-execution) describes five independent attack paths, not a chain: "Each one of the five nginx vulnerabilities are independent attack paths and do not need to be chained together. They differ in what configuration is affected."

CVE-2026-123007, HTTP/2 flow control. This is the one that matters to almost everyone. In the words of the CVE record (https://www.cve.org/CVERecord?id=CVE-2026-123007), "the flow control window can exceed the allowed threshold, potentially resulting in a heap buffer overflow typically followed by an NGINX worker segmentation fault." The record adds that attackers "can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR." The only precondition is HTTP/2 being turned on, and the bug has been there since nginx first shipped HTTP/2 in 1.9.5.

The other four each need a particular configuration:

CVE	Where	Reachable when	nginx severity	Vulnerable versions
CVE-2026-123007	HTTP/2 flow control	HTTP/2 enabled	Major	1.9.5 to 1.31.8
CVE-2026-123633	HTTP/2	HTTP/2 clients proxied to a backend, worker low on `worker_connections`	Medium	1.19.7 to 1.31.8
CVE-2026-123634	Resolver	`proxy_pass` with variables, plus SSI or `mirror` subrequests	Medium	0.6.18 to 1.31.8
CVE-2026-121810	HTTP/3	HTTP/3 (QUIC) enabled	Medium	1.25.0 to 1.31.8
CVE-2026-113425	Mail proxy	nginx configured as a mail proxy	Major	0.5.33 to 1.31.8

Sources: nginx security advisories (https://nginx.org/en/security_advisories.html) for severity and versions, the F5-published CVE records for the conditions.

Where "2Root" comes from

On its own, each nginx bug gives an attacker code execution as the nginx worker user, usually `www-data` or `nginx`. Xint found a second bug in the Linux kernel's SCTP code, a use-after-free in the send path that it says was "introduced in Linux v4.15 in 2018". With it, "an attacker already running code as an nginx worker could reliably gain root." Xint also "obtained a root shell on the host in a setup where nginx was running in a Docker container."

As of 18 November, the kernel bug has **no CVE and no fix**, and Xint is holding back its details until there is one. What it has said is the part that matters for defenders: "On many Linux distributions, the SCTP module is installed by default and the kernel loads it automatically the first time a program opens an SCTP socket." A fully patched kernel does not close this. See the mitigations below.

Why This One Hurts More Than the Usual nginx CVE

nginx has had an unusually busy year for advisories, and most of them were fixed on a normal patch cycle without drama. Xint counted 26 by 17 November, against two in all of 2025. Three things make this release different.

It is unauthenticated and needs nothing but HTTP/2. Many of this year's nginx advisories needed a specific directive combination, such as `alias` with `try_files`, or `map` with a regex. CVE-2026-123007 needs only HTTP/2 to be enabled. Xint calls an unauthenticated nginx RCE "a holy grail for security researchers" and points to CVE-2013-2028 as one of the very few previous examples.

The exposed population is enormous. From a Shodan snapshot on 10 November, Xint found 56.7 million hosts identifying as nginx. Of the 11.94 million that reported a version, 98.9% fell inside the vulnerable range. Xint is careful to say that version strings do not prove exposure, since HTTP/2 must be enabled and many distro builds carry backported fixes, but the scale is clear.

Several teams found it independently, with AI help. The CVE record for CVE-2026-123007 credits four separate reporters: Rapid7, Wiz Research, Xint, and Ikotas Labs "using GPT-6 Astra". Xint says a "fully automated Xint scan" found the other four bugs. When four groups find the same bug at once, it is reasonable to assume others have too.

Exploitation So Far

Here is what is solid as of 19 November:

No reported exploitation. None of the five CVEs is in CISA's KEV catalogue (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) (catalogue version 2026.11.18). Tenable (https://www.tenable.com/blog/nginx2root-cve-2026-123007-frequently-asked-questions-about-five-critical-nginx) reports "no reports of threat actors exploiting these CVEs as of November 18."

A public exploit exists, and it is fragile. Rapid7's Stephen Fewer published a proof of concept for CVE-2026-123007 (https://github.com/sfewer-r7/CVE-2026-123007). Its README says it "is only suitable to demonstrate the given RCE exploitation strategy against a local freshly started Docker container" and "will likely fail against a vulnerable NGINX server which has multiple concurrent clients". Rapid7's analysis (https://www.rapid7.com/blog/post/ve-cve-2026-123007-

critical-nginx-http-2-integer-underflow-leads-to-rce-fixed/) explains why: the attack depends on a specific x86-64 glibc `memcpy` path and a large volume of HTTP/2 traffic.

Full exploits are being withheld. Xint says it "intentionally omit[s] the final steps needed to reproduce the full exploits."

Be careful with GitHub. Around twenty repositories each for `CVE-2026-123007` and `nginx2root` appeared within a day. Fake proof-of-concept repositories carrying malware are a familiar pattern after high-profile CVEs. Do not run any of them on a machine you care about.

Fragile exploits improve. Patch as if exploitation were confirmed.

Which nginx Versions Are Fixed

Product	Fixed release
nginx mainline	**1.31.9**
nginx stable	**1.30.7**
NGINX Plus	37.0.8.1 and 37.3.0.1. R33 and later R releases get no fix: move to 37.x
nginx 1.29.x and older	No upstream release. Get the fix from your distro, or upgrade

Both open source releases came out on 18 November (nginx.org (https://nginx.org/)). The same releases also fix five further bugs that are not part of NGINX2Root, including CVE-2026-118899, an infinite loop when reading a request body over TLS 1.3 that nginx rates "major". Distro advisories mostly cover all of them together.

What Your Distro Is Shipping

Most Linux servers do not run nginx from nginx.org. They run their distribution's package, and **distributions backport fixes without changing the upstream version number**. As Xint puts it, "A backport can fix a vulnerability without changing the version reported by `nginx -v`." A Ubuntu 24.04 host reporting `nginx/1.24.0` can be fully patched. What matters is the full package version.

Distribution	Package	Fixed version	Advisory
Ubuntu 26.10	nginx	1.30.4-7ubuntu1.2	USN-9159-1 (https://ubuntu.com/security/notices/USN-9159-1), 19 Nov
Ubuntu 26.04 LTS	nginx	1.28.3-2ubuntu1.13	USN-9159-1
Ubuntu 24.04 LTS	nginx	1.24.0-2ubuntu7.20	USN-9159-1
Ubuntu 22.04 LTS	nginx	1.18.0-6ubuntu14.23	USN-9159-1
Ubuntu 20.04 and older	nginx	ESM builds, Ubuntu Pro only	USN-9159-1
Debian 13 "trixie"	nginx	**Not fixed yet**	Debian tracker (https://security-tracker.debian.org/tracker/CVE-2026-123007)
Debian 12 "bookworm"	nginx	**Not fixed yet**	Debian tracker
RHEL 8, 9, 10	nginx, nginx:1.24, nginx:1.26	**Not fixed yet** (Affected)	Red Hat CVE page (https://access.redhat.com/security/cve/CVE-2026-123007)
AlmaLinux 10	nginx	1.26.3-16.el10_3.1.alma.2	ALSA-2026:A024
AlmaLinux 9	nginx	1.20.1-32.el9_9.1.alma.3	ALSA-2026:A025
Amazon Linux 2023	nginx	1.30.7-1.amzn2023.0.1	ALAS2023-2026-3494 (https://alas.aws.amazon.com/AL2023/ALAS2023-2026-3494.html)
Amazon Linux 2 (nginx1 extra)	nginx	1.30.7-1.amzn2.0.1	ALAS2NGINX1-2026-018 (https://alas.aws.amazon.com/AL2/ALAS2NGINX1-2026-018.html)
Alpine edge, 3.24	nginx	1.30.7-r0	Alpine security tracker (https://security.alpinelinux.org/vuln/CVE-2026-123007)
Alpine 3.23, 3.22	nginx	1.28.3-r8	Alpine secdb
SUSE, openSUSE	nginx	**Not fixed yet** (under analysis)	SUSE CVE page (https://www.suse.com/security/cve/CVE-2026-123007.html)
FreeBSD	nginx, nginx-devel	1.30.7,3 and 1.31.9	VuXML (https://vuxml.freebsd.org/freebsd/vuln.x

Distribution	Package	Fixed version	Advisory
			ml)

Ubuntu

Canonical shipped USN-9159-1 (https://ubuntu.com/security/notices/USN-9159-1) on 19 November, covering every supported release and eight of the ten CVEs in this nginx release, including all five NGINX2Root bugs. The upstream version strings stay at 1.18.0, 1.24.0 and so on; only the Ubuntu revision changes. Releases from 20.04 back are covered through Ubuntu Pro (ESM).

Debian

As of 19 November, Debian's tracker lists bookworm and trixie as **vulnerable**, including the current security archive builds (1.22.1-9+deb12u10 and 1.26.3-3+deb13u10). Only unstable has a fix so far, in 1.30.6-4. Watch the tracker page (https://security-tracker.debian.org/tracker/CVE-2026-123007) for a DSA, and apply the mitigations below until it lands.

RHEL, Rocky Linux and AlmaLinux

Red Hat rates CVE-2026-123007 **Critical** and lists RHEL 8, 9 and 10 as affected across the `nginx` package and the `nginx:1.24` and `nginx:1.26` module streams, with no advisory yet. Check which stream each host has enabled with `dnf module list --enabled nginx`. AlmaLinux did not wait and published its own fixes for AlmaLinux 9 and 10 (ALSA-2026:A025 and ALSA-2026:A024) on 18 November. Rocky Linux rebuilds Red Hat's packages, so expect its fix to follow Red Hat's.

Amazon Linux

Amazon Linux 2023 moved straight to upstream 1.30.7 in ALAS2023-2026-3494. On Amazon Linux 2, nginx comes from the `nginx1` extras topic, fixed in ALAS2NGINX1-2026-018.

Alpine and containers

Alpine edge and 3.24 carry upstream 1.30.7-r0, and 3.22 and 3.23 have the fixes backported into 1.28.3-r8 (per Alpine's security database). The official `nginx` Docker image (https://hub.docker.com/_/nginx) was rebuilt on release day: the `mainline` and `1.31.9` tags on 18 November, the `stable` and `1.30.7` tags early on 19 November. Pull the new image, rebuild anything that uses it as a base, and redeploy. A running container does not pick up a new image on its own.

Kubernetes ingress-nginx and OpenResty

The community ingress-nginx (https://github.com/kubernetes/ingress-nginx) controller was archived in March 2026 and will not get a fix. If you still run it, disable HTTP/2 with `use-http2: "false"` in its ConfigMap and plan the move off it. F5's own NGINX Ingress Controller is a separate product

with its own releases. OpenResty's latest tag as of 19 November is v1.31.8.1, built on the vulnerable nginx 1.31.8.

If You Cannot Patch Right Now

The CVE record for CVE-2026-123007 lists the workaround as "None". These are holding measures from Xint (https://xint.io/blog/nginx2root-remote-code-execution) and Red Hat (https://access.redhat.com/security/cve/CVE-2026-123007) for the hours or days before a fixed package is installed. Each one covers only some of the bugs.

Check what you are exposed to:

```
# Installed nginx packages and versions
dpkg -l 'nginx*' | awk '/^ii/ {print $2, $3}'        # Debian / Ubuntu
rpm -qa 'nginx*' --qf '%{NAME} %{VERSION}-%{RELEASE}\n'  # RHEL family / Amazon /
SUSE

# Is HTTP/2 enabled? (reads the config on disk)
sudo nginx -T 2>&1 | sed 's/#.*//' \
  | grep -nE
'listen[[:space:]].*http2|^[[:space:]]*http2[[:space:]]+on[[:space:]]*;'

# HTTP/3, resolver, mirror and mail usage
sudo nginx -T 2>&1 | sed 's/#.*//' | grep -nE
'quic|http3|resolver|mirror|^[[:space:]]*mail'
```

Disable HTTP/2 (blocks CVE-2026-123007 and CVE-2026-123633). On nginx 1.25.1 and later, set `http2 off;` in every affected server block and remove `http2` from the `listen` lines. On older versions, just remove `http2` from `listen`:

```
listen 443 ssl;
http2 off;
```

Clients fall back to HTTP/1.1, but anything that needs HTTP/2, such as native gRPC, will break.

Disable HTTP/3 (blocks CVE-2026-121810). Remove `quic` listeners, set `http3 off;` and add `add_header Alt-Svc 'clear' always;`.

Remove request-time DNS with subrequests (CVE-2026-123634). Point `proxy_pass` at a fixed `upstream` group rather than a variable, and turn `mirror off;` where you do not need it.

Lock down the mail proxy (CVE-2026-113425). Bind mail listeners to loopback or allow only trusted networks.

Restart, do not just reload. Xint notes that a reload "applies the new configuration only to new connections", and existing HTTP/2 sessions stay on the old workers. After a config change for mitigation, check for `nginx: worker process is shutting down` in `ps` and restart if they linger.

Block the SCTP module on hosts that do not use SCTP. This is the only defence against the root escalation until a kernel fix exists:

```
echo "install sctp /bin/false" | sudo tee /etc/modprobe.d/nginx2root-sctp.conf
lsmod | grep sctp   # if this prints anything, SCTP is already loaded
```

Xint is explicit about the limits: this "does not unload a module that is already loaded, and it does not disable SCTP compiled into the kernel." If `lsmod` shows `sctp`, plan a reboot after adding the file.

Watch what nginx spawns. Xint observes that "a normal nginx worker has no reason to run external programs." A shell or download tool started by the nginx worker user is the clearest sign of a successful attack. Repeated `worker process ... exited on signal 11` lines in `error.log` can indicate failed attempts.

How to Tell Your Fleet Is Actually Patched

nginx has the same trap as PHP did with PHP2Shell (https://patchmon.net/blog/php2shell-cve-2026-109618-cve-2026-109619-php-rce-patch): **a fixed package on disk is not a fixed process in memory.** Four things tend to go wrong:

The package updated, the service did not restart. Xint is clear: "A configuration reload alone does not replace the running executable." On Linux you can see it directly. If the binary was replaced underneath a running master process, its executable link shows as deleted:

```
sudo ls -l /proc/$(cat /run/nginx.pid)/exe
# ... -> /usr/sbin/nginx (deleted)   means the old binary is still running
```

nginx is somewhere you did not look. The reverse proxy in front of an internal tool, the ingress controller, a container image built from `nginx:1.27` six months ago, the appliance with a web UI.

The version string tells you nothing on its own. `nginx/1.24.0` on Ubuntu 24.04 says nothing; `1.24.0-2ubuntu7.20` does. The changelog is the definitive answer on Debian-family systems:

```
apt changelog nginx 2>/dev/null | grep -E 'CVE-2026-123007'
```

> **Your distro has not shipped yet.** Debian, RHEL and SUSE are the obvious examples this week. "No update available" is not the same as "fixed".

Running those checks on one server takes a minute. Running them across two hundred, and keeping the answer current as Debian and Red Hat ship over the coming days, is the actual job.

This is the problem PatchMon (https://patchmon.net/features/patch-management) is built for. Each PatchMon agent reports every installed package, its version, and the updates available for it, including whether an available update is a security update. Search the Packages view for `nginx` and you get every host carrying an nginx package, the version each one has installed, and which still have an update waiting. As Debian and Red Hat release their fixes, they appear there as pending security updates; as each host updates and reports back, it drops off the list. For containers, the Docker integration (https://patchmon.net/features/docker-monitoring) flags containers whose image has an update available, which is how you catch the stale `nginx:*` images. Every update is timestamped, which is the evidence your auditor or customer will ask for afterwards.

If you would like to see that against your own servers, have a look at the PatchMon pricing page (https://patchmon.net/pricing) and start a PatchMon Cloud trial from there. If you would rather self-host, the Community Edition (https://patchmon.net/open-source) is free and open source.

Frequently Asked Questions

Is Ubuntu 24.04 patched for CVE-2026-123007? Yes, since 19 November. The fixed package is `nginx` 1.24.0-2ubuntu7.20 from USN-9159-1 (https://ubuntu.com/security/notices/USN-9159-1). `nginx -v` will still say 1.24.0.

Is Ubuntu 22.04 patched? Yes. The fixed package is 1.18.0-6ubuntu14.23.

Is Debian patched? Not as of 19 November. Bookworm and trixie are listed as vulnerable on Debian's tracker. Use the mitigations above until a DSA is released.

Does RHEL, Rocky Linux or AlmaLinux have a fix? RHEL does not yet; Red Hat lists RHEL 8, 9 and 10 as affected. AlmaLinux 9 and 10 have their own fixes in ALSA-2026:A025 and ALSA-2026:A024.

Am I affected if HTTP/2 is off? Not by CVE-2026-123007 or CVE-2026-123633. You may still be affected by the HTTP/3, resolver or mail proxy bugs if you use those features, so patch anyway.

Is a reload enough after upgrading? No. Restart nginx, or do a supported live binary upgrade. A reload keeps the old executable running.

Does a kernel update fix the root escalation? Not yet. The SCTP kernel bug Xint used has no CVE and no fix as of 18 November. Block the `sctp` module on hosts that do not need it.

Is it being exploited in the wild? No exploitation has been reported, and none of the five CVEs is in CISA KEV as of 19 November. A lab-only public proof of concept exists.

Bottom Line

NGINX2Root is five remotely reachable memory corruption bugs in the most widely deployed web server on the internet, one of which needs nothing more than HTTP/2. The fix is in nginx 1.31.9 and 1.30.7, Ubuntu, Amazon Linux, Alpine and AlmaLinux have packages out, and Debian, RHEL and SUSE users are still waiting.

What to do today:

- **Inventory every nginx:** hosts, containers, ingress controllers and appliances, with full package versions.
- **Update wherever a fix exists, then restart nginx.** Verify by package version or changelog, not `nginx -v`.
- **Where no fix exists yet, disable HTTP/2** (and HTTP/3, mirror or mail proxy where used) until it does.
- **Block the `sctp` kernel module** on hosts that do not need it, since the root escalation has no patch.
- **Rebuild and redeploy container images,** and move off the retired community ingress-nginx.

The teams that get through events like this calmly are the ones who can answer "which servers still run a vulnerable nginx?" in minutes. If you want to see how PatchMon does that, the pricing page (https://patchmon.net/pricing) is the place to start a trial. Either way, get nginx patched and restarted first.

Sources and Further Reading

- nginx.org: Security advisories (https://nginx.org/en/security_advisories.html)
- nginx.org: nginx 1.31.9 and 1.30.7 release announcement (https://nginx.org/)
- CVE-2026-123007 record (https://www.cve.org/CVERecord?id=CVE-2026-123007)
- F5: K000163926 (CVE-2026-123007) (https://my.f5.com/manage/s/article/K000163926)
- Xint: NGINX2Root, new remote code execution vulnerabilities in nginx (https://xint.io/blog/nginx2root-remote-code-execution)
- Rapid7: CVE-2026-123007 analysis (https://www.rapid7.com/blog/post/ve-cve-2026-123007-critical-nginx-http-2-integer-underflow-leads-to-rce-fixed/) and proof of concept (https://github.com/sfewer-r7/CVE-2026-123007)
- Tenable: NGINX2Root FAQ (https://www.tenable.com/blog/nginx2root-cve-2026-123007-frequently-asked-questions-about-five-critical-nginx)
- CISA: Known Exploited Vulnerabilities Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- Ubuntu: USN-9159-1 (https://ubuntu.com/security/notices/USN-9159-1)

Debian security tracker: CVE-2026-123007 (https://security-tracker.debian.org/tracker/CVE-2026-123007)

Red Hat: CVE-2026-123007 (https://access.redhat.com/security/cve/CVE-2026-123007)

Amazon Linux: ALAS2023-2026-3494 (https://alas.aws.amazon.com/AL2023/ALAS2023-2026-3494.html) and ALAS2NGINX1-2026-018 (https://alas.aws.amazon.com/AL2/ALAS2NGINX1-2026-018.html)

SUSE: CVE-2026-123007 (https://www.suse.com/security/cve/CVE-2026-123007.html)

Alpine Linux security tracker: CVE-2026-123007 (https://security.alpinelinux.org/vuln/CVE-2026-123007)

FreeBSD VuXML (https://vuxml.freebsd.org/freebsd/vuln.xml)

Docker Hub: official nginx image (https://hub.docker.com/_/nginx)

PatchMon

ABOUT PATCHMON

The open source Linux patch management platform

PatchMon gives sysadmins one dashboard for patching across Linux and FreeBSD fleets, with Windows supported alongside. Run it as a managed SaaS on PatchMon Cloud (per-host billing, 14-day trial, no fleet minimum) or self-host the AGPLv3 Community Edition on your own infrastructure.

Start a trial: patchmon.net/pricing