CYBERSECURITY RISK ADVISORY

NGINX2Root: Critical Remote Code Execution Flaws in NGINX Web Servers and Proxies (CVE-2026-123007 and Four Others)

All sectors · Web, platform, Kubernetes and infrastructure teams · Any organization running NGINX directly, in containers or ingress controllers, or inside vendor products

ADVISORY ID	PUBLISHED	CLASSIFICATION	SEVERITY
SCA-ADV-2026-004	November 19, 2026 · v1.0	TLP:CLEAR	Critical

STATUS
Public exploit code · not known exploited

Developing situation. This advisory reflects public information as of **November 19, 2026, 12:00 PM Eastern Time**. F5 is still assessing some of its products, and a related Linux kernel flaw has no patch yet, so check F5's and your Linux vendor's advisories before acting. Each fact carries a numbered citation [1] that links to its source in Appendix A, and claims are attributed to the organization that made them. We deliberately leave out exploit details. TLP:CLEAR means this advisory may be shared without restriction.[11]

1. Executive summary

On November 18, 2026, F5 released out-of-band fixes for ten vulnerabilities in **NGINX**, the web server and reverse proxy that fronts a large share of the internet.[1] Five of them, named **NGINX2Root** by the security firm Xint, can let an attacker **run code on the server without logging in**; F5 rates each **9.2 (Critical) under CVSS v4.0** and 8.1 (High) under CVSS v3.1.[2] [7] The lead flaw, **CVE-2026-123007**, affects any NGINX release from 1.9.5 (2015) through 1.31.8 with **HTTP/2 enabled**, even a server that only serves static files.[2] [7] [9] Xint also reports a separate, **unpatched Linux kernel flaw** that turns a foothold in NGINX into full control of the

host, including from inside a Docker container.[7] No attacks have been reported, and none of the five is in CISA's Known Exploited Vulnerabilities catalog, but exploit code for the lead flaw is public.[8] [10]

Bottom line for executives

- **If you run NGINX, check it now.** That includes NGINX inside containers, Kubernetes ingress controllers and F5 products built on it, such as NGINX Ingress Controller, NGINX Gateway Fabric and F5 WAF for NGINX.[2]
- **Update and restart.** Fixed releases are NGINX Open Source 1.30.7 (stable) and 1.31.9 (mainline), and NGINX Plus 37.0.8.1 and 37.3.0.1. A configuration reload does not load the fix; restart NGINX.[2] [8] [9]
- **Workarounds are partial.** Turning off HTTP/2 blocks only the two HTTP/2 flaws; each of the other three needs its own configuration change. F5 lists no mitigation at all for the lead flaw.[2] [7] [8]
- **Harden Linux hosts too.** Until a kernel fix ships, block the kernel's SCTP module on hosts that don't use it; Xint says the unpatched SCTP flaw is how it went from NGINX to root.[7]
- **Real risk depends on configuration.** Version counts overstate exposure; the flaws need features such as HTTP/2, HTTP/3, request-derived proxy targets or the mail proxy. Check what each server actually has enabled.[9]

2. What happened

WHEN (2026)	EVENT	SOURCE
Oct 11	Xint discovered the vulnerabilities and reported them to F5 through HackerOne on October 16.	[7]
Oct 27 – Nov 10	The reports reached F5's NGINX team on October 27; Xint validated F5's patches on November 10.	[7]
Nov 18	F5 published an out-of-band security notification fixing ten NGINX vulnerabilities, including the five NGINX2Root flaws, along with separate BIG-IP issues. NGINX Open Source 1.30.7 and 1.31.9 and NGINX Plus 37.0.8.1 and 37.3.0.1 carry the fixes.	[1] [2] [9]

WHEN (2026)	EVENT	SOURCE
Nov 18	Xint published its research, withholding the final steps to reproduce its exploits and most details of the Linux kernel flaw. Rapid7 published an analysis and a public exploit for CVE-2026-123007.	[7] [8]
Nov 18	Several research teams, including Wiz, Rapid7 and Xint, were credited with finding the HTTP/2 flaws independently.	[2] [3] [9]
Nov 19	Censys counted about 8.8 million NGINX services potentially exposed to CVE-2026-123007, based on version and HTTP/2 support. None of the five flaws was in CISA's KEV catalog.	[9] [10]

3. The vulnerabilities

CVE	WHAT GOES WRONG	EXPOSED WHEN	AFFECTED NGINX OPEN SOURCE
CVE-2026-123007	Integer underflow in HTTP/2 flow control corrupts worker memory	HTTP/2 is enabled on a reachable listener	1.9.5 – 1.30.6, 1.31.0 – 1.31.8
CVE-2026-123633	Use-after-free in HTTP/2 when the worker runs low on connections	HTTP/2 clients are proxied to a backend	1.19.7 – 1.30.6, 1.31.0 – 1.31.8
CVE-2026-123634	Use-after-free in the DNS resolver	A proxied server name contains variables and an SSI or mirror subrequest resolves the same name	1.0.0 – 1.30.6, 1.31.0 – 1.31.8 (0.6.18 – 0.8.55 also affected, no fix)
CVE-2026-121810	Use-after-free in HTTP/3 (QUIC)	HTTP/3 is enabled and requests are proxied to a backend	1.25.0 – 1.30.6, 1.31.0 – 1.31.8
CVE-2026-113425	Use-after-free in the mail proxy	NGINX is configured as a mail proxy	0.5.33 – 1.30.6, 1.31.0 – 1.31.8

Ranges and conditions are from F5's advisories; Xint describes the required configurations in more detail.[2] [3] [4] [5] [6] [7] For all five, F5 says an attacker can crash or corrupt an NGINX worker process and can run code where address space layout randomization (ASLR) is disabled or can be bypassed.[2] [3] [4] [5] [6]

The Linux kernel flaw: Xint reports a use-after-free in the kernel's SCTP subsystem, present since Linux 4.15 (2018), with no CVE or patch as of November 18. In Xint's tests an attacker

running as an NGINX worker could reliably gain root, including escaping a Docker container to the host. Xint is withholding most details until a kernel fix is available.[7] [8]

4. Affected and fixed versions

PRODUCT	FIXED IN	NOTES
NGINX Open Source	`1.30.7` · `1.31.9`	Stable and mainline. Linux distributions ship their own packages and may backport fixes; check your distribution's advisory.[2] [9]
NGINX Plus	`37.0.8.1` · `37.3.0.1`	Covers all five; CVE-2026-123633 alone is also fixed in 37.0.7.1 and 37.2.0.1. F5's tables list no versions of R34 – R36 as known to be vulnerable.[2] [3] [6]
NGINX Ingress Controller	`5.8.0` · `2026-lts-r11`	4.x and 3.x have no fix; F5 recommends moving to a fixed version.[2]
NGINX Gateway Fabric	`2.9.0`	1.x has no fix.[2]
F5 WAF for NGINX	`5.16.2` · `5.14.4`	NGINX App Protect WAF 4.x and 5.x have no fix.[2]
F5 DoS for NGINX	`4.13.0`	NGINX App Protect DoS 4.x has no fix.[2]
NGINX Instance Manager	`2.25.0`	[2]
F5 Distributed Cloud, NGINX One Console	Under review	F5 is still researching these services.[2]
BIG-IP, BIG-IQ, F5OS	Not affected	By these NGINX flaws; F5 fixed separate BIG-IP issues the same day.[1] [2]

For the bundled products, F5 rates the mail-proxy flaw (CVE-2026-113425) lower, 6.9 under CVSS v4.0, and the other four 9.2.[2] [6]

5. Exploitation and exposure

- **Not known exploited:** as of November 18, Tenable reported no exploitation in the wild and no listing in CISA's KEV catalog; our check of the catalog on November 19 found none of the five.[8] [10]

- **Public exploit code:** Rapid7 released a proof of concept for CVE-2026-123007 with a full remote code execution exploit, demonstrated against NGINX 1.31.8 in Docker. Rapid7 describes it as constrained: it depends on a particular x86-64 system library, needs about 128 GB of HTTP/2 traffic and must defeat ASLR.[8]
- **Working exploits withheld:** Wiz demonstrated remote code execution through both HTTP/2 flaws and Xint through all five in its test setups; neither has published its exploits.[7] [8] [9]
- **Exposure estimates vary:** Censys counted about 8.8 million NGINX services potentially exposed to CVE-2026-123007 on November 19, more than 511,000 already patched or mitigated, and 104 million more that don't disclose a version. Researcher Florian Roth cautions that the flaws need non-default configurations and that counts based on version numbers alone are misleading; in his small sample about 66% of NGINX HTTPS endpoints supported HTTP/2.[9]

9.2	~8.8 million	2015
CVSS v4.0 score F5 assigns each of the five flaws[2]	NGINX services potentially exposed to the lead flaw, per Censys (Nov 19)[9]	the lead flaw has been present since NGINX 1.9.5[2]

These counts use different methods and mostly rely on what servers advertise. They show the scale of potential exposure, not confirmed vulnerable or compromised systems.[9]

6. Business risk

- **Your front door:** NGINX usually sits in front of websites, APIs and applications. A takeover there can expose traffic passing through it, including credentials and session data, and give an attacker a path into internal systems. (Our assessment.)
- **Containers are not a boundary here:** Xint reports escaping a Docker container to root on the host by chaining an NGINX flaw with the unpatched kernel flaw. Kubernetes ingress controllers built on NGINX are affected products.[2] [7]
- **Outages even without a breach:** F5 says every one of these flaws can crash NGINX worker processes, which can mean dropped connections or downtime.[2] [3] [4] [5] [6]
- **Hidden in vendor products:** appliances, control panels and hosting platforms often bundle NGINX, so exposure may sit with suppliers. (Our assessment.)

7. Recommended actions

Today

1. **Find every NGINX instance**, starting with internet-facing ones: servers, container images, Kubernetes ingress controllers and vendor products.
2. **Update** NGINX Open Source to 1.30.7 or 1.31.9, or NGINX Plus to 37.0.8.1 or 37.3.0.1, and F5 NGINX products to the fixed versions above, then **restart** NGINX; a reload does not replace the running program.[2] [8]
3. **If you can't patch today,** apply the workaround for each feature you use: turn off HTTP/2 (covers CVE-2026-123007 and CVE-2026-123633); remove HTTP/3 listeners (CVE-2026-121810); avoid proxied server names with variables combined with SSI or mirror (CVE-2026-123634); restrict mail proxy listeners to trusted networks (CVE-2026-113425). None of these replaces patching.[4] [6] [7] [8]
4. **Block the SCTP kernel module** on Linux hosts that don't need it, as Xint advises, until your Linux vendor ships a fix. Xint notes this does not unload a module already loaded or disable SCTP built into the kernel.[7]
5. **Ask your hosting providers and vendors** (CDNs, control panels, appliances, managed Kubernetes) whether they have updated.

Within 72 hours

1. **Rebuild and redeploy container images** that include NGINX, and confirm ingress controllers run fixed versions.
2. **Plan replacements** for products F5 lists without a fix (NGINX App Protect WAF and DoS, Ingress Controller 3.x and 4.x, Gateway Fabric 1.x).[2]
3. **Check logs** on servers exposed before patching for repeated worker crashes, unusual HTTP/2 traffic volumes and unexpected processes started by NGINX workers.
4. **If you find signs of compromise,** treat it as an incident: preserve evidence, contain, engage incident response support, and check notification obligations.

Strategic

1. **Keep ASLR on** everywhere: F5 says code execution depends on ASLR being disabled or bypassed.[2]
2. **Turn off protocols and features you don't use** (HTTP/3, mail proxy, SSI), which shrinks exposure to the next flaw.

3. **Keep a live inventory of components**, including what is inside container images and vendor products, so the next zero-day can be scoped in hours.
4. **Track CISA's KEV catalog**, and be ready to move faster if any of these flaws is added.[10]

8. What to watch for

- Repeated NGINX worker crashes in the error log (for example, worker processes exiting on a segmentation fault), especially in bursts.
- Very large volumes of HTTP/2 traffic from a single source; Rapid7's public exploit needs about 128 GB.[8]
- NGINX worker processes starting shells or other programs, or making unexpected outbound connections.
- The SCTP kernel module loaded on hosts that don't use it.
- New entries in CISA's KEV catalog for any of the five CVEs, and a Linux kernel advisory for the SCTP flaw Xint described.[7] [10]

9. Questions for leadership

1. Do we know every place NGINX runs, including containers, ingress controllers and vendor products?
2. Are internet-facing NGINX servers patched and restarted, or protected by workarounds, today, and who confirmed it?
3. Which of our suppliers and hosting providers have confirmed they are patched?
4. Are any of our F5 NGINX products on versions without a fix, and what is the replacement plan?
5. Have we blocked the SCTP kernel module on hosts that don't need it?

Appendix A. Source map

Every citation, traced to its publisher. Sources were opened and checked on November 19, 2026, and the advisory was fact-checked independently before publishing.

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
1	Out-of-band security notification (Nov 18, 2026), read Nov 19: index of ten NGINX CVEs and separate BIG-IP issues, with affected products per CVE	F5, K000164058	Vendor (official)	my.f5.com
2	CVE-2026-123007 (Nov 18, 2026), read Nov 19: description; heap overflow in HTTP/2 flow control; code execution when ASLR is disabled or bypassed; CVSS v3.1 8.1, v4.0 9.2; CWE-191; affected and fixed versions for NGINX Open Source, NGINX Plus and other F5 products; products not affected or under review; mitigation "None"; researcher acknowledgments	F5, K000163926	Vendor (official)	my.f5.com
3	CVE-2026-123633 (Nov 18, 2026), read Nov 19: use-after-free with HTTP/2 proxying when low on worker connections; affected and fixed versions (NGINX Plus also 37.0.7.1 and 37.2.0.1); mitigation "None"; acknowledgments	F5, K000163928	Vendor (official)	my.f5.com
4	CVE-2026-123634 (Nov 18, 2026), read Nov 19: resolver use-after-free with variable proxied server names and SSI or mirror subrequests; affected versions incl. 0.6.18 – 0.8.55 without fix; mitigation: avoid SSI or mirror with variable server names	F5, K000163925	Vendor (official)	my.f5.com
5	CVE-2026-121810 (Nov 18, 2026), read Nov 19: HTTP/3 use-after-free; conditions beyond the attacker's control; affected and fixed versions; mitigation "None"	F5, K000163927	Vendor (official)	my.f5.com
6	CVE-2026-113425 (Nov 18, 2026), read Nov 19: mail proxy use-after-free; affected versions from 0.5.33; NGINX Plus fixed in 37.0.8 and 37.3.0; bundled products rated CVSS v4.0 6.9; mitigation: restrict listeners to trusted networks	F5, K000163931	Vendor (official)	my.f5.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
7	"NGINX2Root" research (Nov 18, 2026, modified Nov 19): naming; the five CVEs and required configurations; working exploits in tested setups; Linux kernel SCTP flaw (since 4.15, unpatched, root and container escape); disclosure timeline; per-flaw workarounds; SCTP module block and its limits; exploit details withheld	Xint (Theori)	Security researcher	xint.io
8	NGINX2Root FAQ (Nov 18, 2026): no exploitation reported and not in KEV as of Nov 18; Rapid7 public proof of concept for CVE-2026-123007 and its constraints (x86-64 library dependency, ~128 GB of HTTP/2 traffic, ASLR); Wiz confirmed exploits but did not publish them; restart rather than reload; workaround coverage; no CVE for the kernel flaw as of Nov 18	Tenable	Security vendor	tenable.com
9	"Critical NGINX 'NGINX2Root' bugs let attackers hijack servers" (Bill Toulas, Nov 19, 2026), read Nov 19: researchers credited; affected ranges of the HTTP/2 flaws; Wiz RCE demos; fixed versions; Censys exposure (about 8.8 million potentially exposed, more than 511,000 patched or mitigated, 104 million undisclosed versions, as of Nov 19); Florian Roth's caution on non-default configurations; ~66% HTTP/2 support in his sample	BleepingComputer	Security news	bleepingcomputer.com
10	KEV catalog version 2026.11.18, checked Nov 19 via CISA's official kev-data repository: none of CVE-2026-123007, -123633, -123634, -121810 or -113425 listed	CISA Known Exploited Vulnerabilities catalog, via official kev-data repository	U.S. government	github.com/cisagov
11	TLP:CLEAR definition; Traffic Light Protocol 2.0	FIRST	Standards body	first.org

Strat Cyber Advisors · Advisory SCA-ADV-2026-004 · v1.0 · Published November 19, 2026 · **TLP:CLEAR**

This advisory summarizes public information for awareness and planning. It is not legal advice and does not replace guidance from your vendors or incident responders. Need help assessing exposure? Contact advisors@stratcyberadvisors.com.