CHECK POINT

EXPOSURE MANAGEMENT

CHECK POINT EXPOSURE MANAGEMENT RESEARCH

NGINX HTTP/2: Two Critical RCE Flaws

How two memory-corruption bugs in NGINX's HTTP/2 code let an unauthenticated attacker run code on the server in front of your websites and APIs.

CVE-2026-123007 · CVE-2026-123633

November 18, 2026

Critical

Unauthenticated RCE

INSIDE THIS ADVISORY

Contents

01 **Executive Summary** 3
Our Recommendation 3
02 **At a Glance** 4
03 **How the Flaws Work** 5
Current Limits on Attackers 5
04 **Exposure and Scope** 6
Are You Affected? 6
Where NGINX Hides 7
05 **Remediation** 8
Fixed Versions 8
Temporary Mitigation 8
Three More Critical Flaws 9
06 **Recommended Action Plan** 10
07 **Detection and Hunting** 11
08 **Timeline** 11
→ **Contact Us** 12

PUBLISHED BY
Check Point Exposure Management Research Team

DATE
November 18, 2026

THREAT TYPE
Remote code execution · Memory corruption

SOFTWARE AFFECTED
NGINX Open Source and NGINX Plus

© 2026 Check Point Software Technologies Ltd. All rights reserved.

OVERVIEW

01 Executive Summary

The server that sits in front of your websites and APIs can now be taken over with no login and no flaw in your own code.

CVE-2026-123007 and CVE-2026-123633 are two critical memory-corruption flaws in how NGINX handles HTTP/2 traffic. NGINX is the world's most widely used web server. It typically terminates HTTPS and routes requests to the applications and APIs behind it, so one compromised NGINX server can put several services at risk at once.

Both flaws need HTTP/2 to be enabled, which is common on modern HTTPS sites. CVE-2026-123007 affects every NGINX release since HTTP/2 support arrived in 2015, and researchers ran code on a server that only served static files, with no backend application and no third-party modules. CVE-2026-123633 affects NGINX acting as a reverse proxy when it runs low on connection slots.

9.2	2015	1	0
CVSS v4.0 score assigned by F5 to each flaw	Year the oldest flaw entered NGINX, with version 1.9.5	Public proof-of-concept exploit already released	Confirmed attacks in the wild as of November 18, 2026

F5 and the NGINX project released fixes on November 18, 2026. At least five research teams found these flaws independently, several with AI-assisted tooling, and working exploit code for CVE-2026-123007 is already public. The same release also fixes three more critical NGINX flaws that turning off HTTP/2 doesn't block, covered in section 05.

OUR RECOMMENDATION

Upgrade internet-facing NGINX servers with HTTP/2 enabled to 1.30.7 or 1.31.9 now, or NGINX Plus 37.0.8.1 or 37.3.0.1. If you can't upgrade today, turn off HTTP/2 on those listeners. Then extend the work to internal servers, containers, ingress controllers, and appliances that bundle NGINX.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

AT A GLANCE

02 Key Facts

CVE IDS

CVE-2026-123007 · CVE-2026-123633

Part of a set of five critical NGINX flaws publicly called NGINX2Root

SEVERITY

Critical

CVSS v4.0 9.2 and CVSS v3.1 8.1 (F5) for both flaws. Red Hat rates CVE-2026-123007 Critical

FLAW TYPE

HTTP/2 memory corruption

A flow-control integer underflow that leads to an out-of-bounds copy, and a connection use-after-free

AUTHENTICATION

None required

An attacker only needs to open an HTTP/2 connection to the server

AFFECTED

NGINX 1.9.5 to 1.31.8

CVE-2026-123633 starts at 1.19.7. NGINX Plus 37.x before the fixed builds, and R34 to R36, which get no fix

KEY CONDITION

HTTP/2 enabled

Any HTTP/2 listener for CVE-2026-123007. HTTP/2 plus requests passed to a backend for CVE-2026-123633

FIX STATUS

Available

NGINX 1.30.7 and 1.31.9; NGINX Plus 37.0.8.1 and 37.3.0.1. Many Linux distribution packages are still pending

EXPLOITATION

None confirmed

As of November 18, 2026. A public exploit exists for CVE-2026-123007. Not in the CISA KEV catalog

BOTTOM LINE

Patch internet-facing NGINX with HTTP/2 first

These servers are the front door to your applications. Where you can't patch today, turning off HTTP/2 blocks both flaws until you can

© 2026 Check Point Software Technologies Ltd. All rights reserved.

TECHNICAL ANALYSIS

03 How the Flaws Work

HTTP/2 lets many requests, called streams, share one connection. NGINX tracks how much data it may send on that connection with a flow-control counter. CVE-2026-123007 breaks that accounting.

STEP 1
HTTP/2 session
TLS connection using h2

▶

STEP 2
Window abuse
Cancels and window updates

▶

STEP 3
Counter wraps
A bounds check fails

▶

STEP 4
Bad copy
Out-of-bounds memory copy

▶

RESULT
Code execution
Runs as the NGINX worker

CVE-2026-123007

Flow-control integer underflow

A canceled stream's refund pushes the flow-control counter past its limit, so a later check wraps around and an invalid length becomes an out-of-bounds copy. Since NGINX 1.9.5.

CVE-2026-123633

Connection use-after-free

A busy connection stays on the list of connections safe to close. When proxying runs low on slots, NGINX frees it mid-request and keeps using the memory. Since NGINX 1.19.7.

1. **Remote code execution** · No login

   Commands run as the NGINX worker, even on servers that only serve static files. Failed attempts crash workers.

2. **Data theft across applications** · Shared front door

   Traffic, credentials, and secrets for every site and API behind that NGINX are exposed.

3. **Path to root** · Linux kernel chain

   Researchers chained a separate, unpatched Linux SCTP flaw to reach root and escape a container.

REALITY CHECK

Current limits on attackers

The public exploit needs about 128 GB of HTTP/2 traffic on one connection and an AVX-512 processor, and likely fails through a proxy. That slows mass attacks, not targeted ones.

DON'T RELY ON

ASLR, WAF rules, or access logs

Researchers defeated ASLR by leaking memory first. WAF rules don't inspect the HTTP/2 control frames involved, and access logs don't record them.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

EXPOSURE

04 Exposure and Scope

Are You Affected?

A server is exposed when all three conditions are true.

CONDITION	AFFECTED	NOT AFFECTED
NGINX version	NGINX Open Source 1.9.5 to 1.30.6 and 1.31.0 to 1.31.8 (CVE-2026-123633 from 1.19.7). NGINX Plus 37.x before 37.0.8.1 or 37.3.0.1, and NGINX Plus R34 to R36	NGINX 1.30.7, 1.31.9, and later; NGINX Plus 37.0.8.1 and 37.3.0.1. F5 BIG-IP, BIG-IQ, and F5OS are not affected
HTTP/2	Any listener that accepts HTTP/2 (CVE-2026-123007). HTTP/2 with requests passed to a backend through proxy_pass, fastcgi_pass, or grpc_pass (CVE-2026-123633)	HTTP/2 disabled on every listener
Reachability	An attacker can open an HTTP/2 connection to NGINX directly, through TLS passthrough, or through a front end that speaks HTTP/2 to NGINX	A front end terminates HTTP/2, forwards HTTP/1.1, and direct access is blocked. This lowers risk but doesn't replace patching

Check the version and whether HTTP/2 is configured on the server, then confirm from outside whether the server offers HTTP/2. If the second command prints `ALPN protocol: h2`, HTTP/2 is on.

ON THE SERVER

```
nginx -v; grep -rnwE 'http2' /etc/nginx/
```

FROM OUTSIDE

```
openssl s_client -connect <host>:443 -alpn h2 </dev/null 2>/dev/null | grep ALPN
```

BEFORE YOU CLOSE ANY FINDINGS

Don't trust the version string alone. Linux distributions often backport fixes without changing the version number, so check your vendor's advisory. **Look for bundled copies.** NGINX inside appliances, ingress controllers, and container images isn't fixed by operating system updates.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Where NGINX Hides

NGINX runs in far more places than a dedicated web server. Here's where to look and what to do in each case. Vendor status is as of November 18, 2026.

DEPLOYMENT	WHAT WE KNOW	WHAT TO DO
Linux distribution packages FIXES PENDING	Ubuntu 24.04 (1.24.0), Ubuntu 22.04 (1.18.0), and Debian 12 (1.22.1) all ship affected versions. Ubuntu and Red Hat fixes are still pending, and fixes may be backported without a version change	Turn off HTTP/2 on internet-facing listeners now, and watch for your distribution's security update
Official Docker images FIXED TAGS AVAILABLE	Fixed tags such as 1.31.9, 1.30.7, and 1.31.9-alpine are published. Generic tags can lag behind, and restarting a container keeps its old image	Pin an explicit fixed tag, rebuild every image built on top of NGINX, and redeploy
Kubernetes ingress-nginx NO UPSTREAM FIX	Vulnerable to CVE-2026-123633. The community project was retired in March 2026 and won't ship a fix	Turn off HTTP/2 in the controller's configuration as a stopgap, and plan a move to a maintained ingress controller
NGINX Plus R34 to R36 NO FIX	F5 lists these releases as vulnerable with no fixed build	Move to NGINX Plus 37.0.8.1 or 37.3.0.1. Until then, turn off HTTP/2
Appliances and bundled products VENDOR DEPENDENT	Products that ship NGINX need a fix from their own vendor. Widespread attacks often start with packaged products that share an identical build	Ask each vendor for its fix date, and turn off HTTP/2 where the product allows it
Behind a CDN or WAF LOWER RISK, NOT SAFE	A front end that terminates HTTP/2 may block these attacks. WAF rules don't inspect the HTTP/2 control frames involved	Block direct access to the origin server, and patch it anyway

ONE RULE FOR EVERYTHING ELSE

Internal NGINX counts too. An attacker who already has a foothold inside your network can use these flaws to move laterally, so internal reverse proxies, load balancers, and ingress controllers belong in the same patch plan.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

REMEDIATION

05 Fix and Mitigate

Fixed Versions

Upgrading NGINX is the only complete fix. The table reflects vendor status as of November 18, 2026. Always confirm against your vendor's own advisory.

PRODUCT	FIXED RELEASE	NOTES
NGINX Open Source (stable)	1.30.7	Fixes both flaws
NGINX Open Source (mainline)	1.31.9	Fixes both flaws
NGINX Plus 37.x	37.0.8.1 · 37.3.0.1	37.0.7.1 and 37.2.0.1 fix only CVE-2026-123633. Use 37.0.8.1 or 37.3.0.1 to fix both
NGINX Plus R34 to R36	No fix	Upgrade to a fixed 37.x build
Ubuntu, all supported releases	Not yet released	Fix marked as needed
Red Hat Enterprise Linux 8, 9, 10	Not yet released	Under investigation
Debian, Amazon Linux, SUSE	Not yet published	Check vendor advisories
F5 BIG-IP, BIG-IQ, F5OS	Not affected	No action needed for these flaws

Temporary Mitigation

Can't upgrade today? Turn off HTTP/2 on affected listeners, reload, and turn it back on after upgrading. This blocks both flaws.

NGINX VERSION	WHAT TO CHANGE	THINGS TO KNOW
1.25.1 and later	Set `http2 off;` in each affected server block, and remove `http2` from any `listen` directive	Most clients fall back to HTTP/1.1. gRPC needs HTTP/2 and will break, so patch those services instead
Before 1.25.1	Remove `http2` from every `listen` directive	Test application compatibility before changing production

DON'T SKIP THESE STEPS

A reload applies a configuration change but keeps the old binary, so restart NGINX after upgrading. After any change, confirm the old workers have exited, then rerun the outside check to verify HTTP/2 is off. Turning off HTTP/2 doesn't cover the other flaws fixed in the same release.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Three More Critical Flaws in the Same Release

The two HTTP/2 flaws are part of a set of five critical NGINX vulnerabilities, publicly called NGINX2Root. Each of the other three is an independent path to unauthenticated code execution, rated CVSS v4.0 9.2 by F5, and turning off HTTP/2 doesn't block any of them. NGINX 1.30.7 and 1.31.9 fix all five, along with five lower-severity issues. If you can't upgrade yet, use the workaround for each feature you run.

CVE AND FLAW	EXPOSED WHEN	WORKAROUND
CVE-2026-123634 DNS resolver use-after-free	`resolver` is set and a `proxy_pass` uses a variable (for example, `http://$host`). Subrequest features such as `mirror` or SSI may reach it, so turning off `mirror` alone isn't enough	Point `proxy_pass` at a fixed upstream group, removing request-time DNS lookups
CVE-2026-121810 HTTP/3 (QUIC) use-after-free	HTTP/3 is enabled and requests are passed to a backend	Remove QUIC listeners and set `http3 off;`
CVE-2026-113425 Mail proxy use-after-free	The mail proxy runs with `proxy on` and `auth_http`	Bind mail proxy listeners to a loopback address, or allow only trusted IP addresses at the firewall

CLOSE THE PATH TO ROOT

Any of the five NGINX flaws can be chained with an unpatched use-after-free in the Linux kernel's SCTP code, present since Linux 4.15 in 2018, to gain root and escape a Docker container. Until a kernel fix ships, block the SCTP module where you don't need it by adding `install sctp /bin/false` to a file in `/etc/modprobe.d/`. This doesn't unload a module already in use.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

WHAT TO DO NEXT

06 Recommended Action Plan

01 **Find every NGINX**
Include hosts, container images, Kubernetes ingress controllers, load balancers, appliances, and origin servers behind your CDN.

02 **Check HTTP/2 from outside**
Run the external check against each internet-facing host. Servers that offer HTTP/2 go to the top of the list.

03 **Patch internet-facing HTTP/2 first**
Upgrade to NGINX 1.30.7 or 1.31.9, or NGINX Plus 37.0.8.1 or 37.3.0.1. Then move on to internal servers.

04 **Mitigate where you must wait**
Turn off HTTP/2 on servers still waiting on a fix, except gRPC services, and apply the workarounds for the other three flaws.

05 **Restart and verify**
Restart rather than reload, rebuild container images, and confirm with `nginx -v` and the external HTTP/2 check.

06 **Harden the host**
Block the SCTP kernel module where it isn't needed, and limit what the NGINX worker account can read.

07 **Respond if you find signs of attack**
Isolate the host, rotate secrets the worker could reach, including TLS private keys, and rebuild from a trusted image.

08 **Remember one rule**
A reload isn't an upgrade. Restart NGINX.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

HUNTING

07 Detection and Hunting

These signals can point to exploitation attempts. None of them proves a compromise, and their absence doesn't prove a server is safe.

ERROR LOG

Repeated worker crashes

NGINX worker processes exiting on a signal, especially in bursts

HOST

Unexpected child processes

NGINX workers starting shells or other programs, or opening new outbound connections

NETWORK

Huge, long-lived HTTP/2 sessions

Single HTTP/2 connections that stay open and move unusually large volumes of data

PROTOCOL

Control-frame floods

Very high rates of HTTP/2 WINDOW_UPDATE or RST_STREAM frames, where your tools can see them

TIMELINE · 2026

08 Chronology

OCTOBER 16, 2026

The first research team reports the NGINX flaws to F5.

OCTOBER 21, 2026

A second team reports the use-after-free, later CVE-2026-123633. F5 confirms it was already reported.

NOVEMBER 10–16, 2026

F5 shares patches for review. More teams report the flow-control flaw, and CVE-2026-123007 is assigned.

NOVEMBER 18, 2026

F5 and NGINX release fixes. A public exploit for CVE-2026-123007 appears, and national CERTs in Japan, Poland, and France issue alerts. No confirmed exploitation, and neither CVE is in the CISA KEV catalog.

This advisory reflects information available as of November 18, 2026. Details may change as vendors publish fixes and as threat activity develops. It is provided for information only and does not replace guidance from your software vendors.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

CHECK POINT

EXPOSURE MANAGEMENT

Contact Us

UAE

202 - 204, Building 15
Dubai Internet City, UAE

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1
Singapore 079120

PHILIPPINES

Tel: +63-2-8465-9200
Unit 2005, 20th Floor, Zuellig Building, Makati Avenue,
corner Paseo de Roxas, Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44-20-7628-4211
85 London Wall, 4th Floor
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F, 1-2-8, Toranomon,
Minato-ku, Tokyo 105-0001

For more information visit: **checkpoint.com**

© Check Point, 2026. All Rights Reserved.