Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

NGINX2Root: From an Unauthenticated HTTP/2 Request to Root on the Host

Date of Publication	Admiralty Code	TA Number
November 19, 2026	A1	TA2026346

Summary

First Seen: November 18, 2026 (coordinated public disclosure)
Affected Products: F5 NGINX Open Source, F5 NGINX Plus
Impact: F5 has fixed five NGINX flaws that are named NGINX2Root. The two with the widest reach are CVE-2026-123007, where NGINX loses count of how much data a client has allowed it to send over HTTP/2, and CVE-2026-123633, where NGINX frees a connection's memory while a request is still using it. Both let an attacker with no login run code on the server, and both need HTTP/2 switched on. The other three, CVE-2026-123634, CVE-2026-121810, and CVE-2026-113425, can also lead to code execution, but each needs a particular setup. CVE-2026-123007 has been in the code since 2015, making it about ten years old. F5 disclosed the vulnerabilities and released fixes on November 18, 2026. Update affected NGINX deployments to the latest release, which includes multiple security fixes.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-123007	nginx2root (NGINX HTTP/2 send_window Integer Underflow Remote Code Execution Vulnerability)	F5 NGINX Open Source, F5 NGINX Plus	✗	✗	✓
CVE-2026-123633	nginx2root (NGINX HTTP/2 Connection Use-After-Free Remote Code Execution Vulnerability)	F5 NGINX Open Source, F5 NGINX Plus	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-123634	nginx2root (NGINX Resolver Memory Corruption Remote Code Execution Vulnerability)	F5 NGINX Open Source, F5 NGINX Plus	✗	✗	✓
CVE-2026-121810	nginx2root (NGINX HTTP/3 Use-after-Free Vulnerability)	F5 NGINX Open Source, F5 NGINX Plus	✗	✗	✓
CVE-2026-113425	nginx2root (NGINX Mail Proxy Use-after-Free Vulnerability)	F5 NGINX Open Source, F5 NGINX Plus	✗	✗	✓

Vulnerability Details

#1

NGINX2Root is the name given to a set of five NGINX vulnerabilities disclosed on November 18, 2026. The lead flaw, CVE-2026-123007, is a memory corruption bug in the way NGINX handles HTTP/2 connections, classified as CWE-191, an integer underflow. The second flaw covered in this advisory, CVE-2026-123633, is a use-after-free, where memory belonging to a connection is released while a request still needs it. F5 scores all five at 9.2 under CVSS v4.0, placing them in the Critical band on the newer scoring system, and the same NGINX releases fix every one of them.

#2

CVE-2026-123007 sits in HTTP/2 flow control, where a client tells the server how much response data it is ready to receive. NGINX tracks that allowance in a counter that cannot hold negative numbers. If a client stops reading so data piles up, then cancels the request at the right moment, NGINX gives the allowance back without checking the limit, and the counter ends up holding a value the rest of the code never expects. The next safety check wraps around, and NGINX believes it has almost unlimited room to send. That bad number later becomes a negative length, and NGINX copies memory well outside the area it should touch. From there, an attacker can leak memory addresses, overwrite data, and run code.

#3

CVE-2026-123633 follows a different route to the same outcome. NGINX keeps a list of connections it can close when it needs room for new ones. An HTTP/2 connection can join that list while it has no active requests, but a bug means it is not removed once a request actually starts. If free connection slots run low, NGINX can pick that connection to close while it is still processing a live request. The close path frees the connection's memory, processing resumes on the original request using pointers into memory that has already been released, and the freed space can be filled with attacker-influenced data. This one is reachable only when NGINX is passing requests to a backend server, and the worker is running short on connections, which makes it narrower than CVE-2026-123007 but still remotely triggerable without authentication.

#4

The other three flaws in the set, and F5 says each can lead to code execution under the same ASLR condition as CVE-2026-123007. CVE-2026-123634 is a resolver flaw that needs a proxied server name built from variables, together with a server-side include or mirror subrequest to a location that looks up the same name. CVE-2026-121810 needs HTTP/3 to be switched on. CVE-2026-113425 applies only where NGINX is used as a mail proxy. Because none of the three depends on HTTP/2, turning HTTP/2 off does nothing for them, and F5 publishes configuration workarounds only for the resolver and mail proxy flaws. NGINX Open Source 1.30.7 and 1.31.9 fix all five.

#5

In scope, CVE-2026-123007 affects unpatched NGINX Open Source from 1.9.5 through 1.31.8, and CVE-2026-123633 affects 1.19.7 through 1.31.8. NGINX Plus is affected in 37.0.0 before 37.0.8.1, 37.1.0 before 37.3.0.1, and the R34 to R36 branch, for which F5 lists no fix. Releases before 1.9.5 predate HTTP/2 support, and builds compiled without the HTTP/2 module are out of scope. F5 lists BIG-IP, BIG-IQ, and F5OS as not vulnerable. Scoping needs care in two places: distributions often backport a fix without changing the version number NGINX reports. The community ingress-nginx project was archived in March 2026 and will ship no further security fixes, which leaves anyone still running it needing a migration plan.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-123007	F5 NGINX Open Source (1.9.5 through 1.31.8), F5 NGINX Plus (37.0.0 before 37.0.8.1; 37.1.0 before 37.3.0.1; R34 through R36)	cpe:2.3:a:f5:nginx:*:*:*:*:open_source:*:*:* cpe:2.3:a:f5:nginx_plus:*:*:*:*:*:*:*:*	CWE-191 CWE-787
CVE-2026-123633	F5 NGINX Open Source (1.19.7 through 1.31.8), F5 NGINX Plus (37.0.0 before 37.0.7.1; 37.1.0 before 37.2.0.1; R33 and later R-series)	cpe:2.3:a:f5:nginx:*:*:*:*:open_source:*:*:* cpe:2.3:a:f5:nginx_plus:*:*:*:*:*:*:*:*	CWE-416
CVE-2026-123634	F5 NGINX Open Source (before 1.30.7 / 1.31.9; F5 NGINX Plus (before 37.0.8.1 / 37.3.0.1)	cpe:2.3:a:f5:nginx:*:*:*:*:open_source:*:*:* cpe:2.3:a:f5:nginx_plus:*:*:*:*:*:*:*:*	CWE-416
CVE-2026-121810	F5 NGINX Open Source (before 1.30.7 / 1.31.9; F5 NGINX Plus (before 37.0.8.1 / 37.3.0.1)	cpe:2.3:a:f5:nginx:*:*:*:*:open_source:*:*:* cpe:2.3:a:f5:nginx_plus:*:*:*:*:*:*:*:*	CWE-416
CVE-2026-113425	F5 NGINX Open Source (before 1.30.7 / 1.31.9; F5 NGINX Plus (before 37.0.8.1 / 37.3.0.1)	cpe:2.3:a:f5:nginx:*:*:*:*:open_source:*:*:* cpe:2.3:a:f5:nginx_plus:*:*:*:*:*:*:*:*	CWE-416

Recommendations

Patch NGINX Without Delay: Updating is the only complete fix. Move NGINX Open Source to 1.30.7 on the stable branch or 1.31.9 on mainline, as both releases address all five NGINX2Root flaws. For NGINX Plus, move to 37.0.8.1 or 37.3.0.1. If you are on the R34 to R36 branch or an older open-source branch with no fixed build listed, plan a migration to a fixed 37.x or 1.30.7/1.31.9 release instead of waiting for a backport.

Restart NGINX After Updating: A configuration reload is not enough. Reloading applies new settings but leaves the old program running in memory, so the flaw stays live until the service is fully restarted or a live binary upgrade is performed. Existing connections can otherwise remain attached to old worker processes carrying the vulnerable code.

Turn Off HTTP/2 If You Cannot Patch Today: On NGINX 1.25.1 and later, set `http2 off;` in each affected server block and remove the `http2` parameter from its listen directives. On 1.9.5 through 1.25.0, remove `http2` from the listen directive so that `listen 443 ssl http2;` becomes `listen 443 ssl;`. Clients will fall back to HTTP/1.1, and services that depend on HTTP/2, such as gRPC, will stop working, so test compatibility before rolling this out. This covers CVE-2026-123007 and CVE-2026-123633 only and is a temporary measure, not a replacement for the patch.

Confirm Your Real Exposure: Check whether the build includes HTTP/2 and whether the configuration actually enables it, then test from outside the network to see whether HTTP/2 is reachable over the internet. If a CDN or load balancer terminates HTTP/2 in front of NGINX, an external test only reaches that device, so test the NGINX origin port directly. Do not rely on the reported version number alone, because distributions patch without changing it.

Close the Privilege Escalation Path: Code execution lands with the worker process's permissions, so reaching root needs a second flaw. Patch known local privilege escalation issues on NGINX hosts with the same urgency as the NGINX update itself. The newly reported Linux kernel SCTP flaw has no patch available, so on hosts that do not use SCTP, block the kernel module from loading. Note that blocking the module does not unload one already loaded or disable SCTP compiled into the kernel.

Cover the Other Three Flaws Separately: Turning off HTTP/2 does nothing for CVE-2026-123634, CVE-2026-121810, or CVE-2026-113425, so each needs its own temporary step where patching has to wait. For the resolver flaw, avoid SSI and mirror directives and do not build a proxied server name from variables. For the HTTP/3 flaw, turn HTTP/3 off where it is enabled. For the mail proxy flaw, limit the mail listeners to trusted networks. F5 publishes workarounds for only two of the five flaws, so treat these as risk reduction rather than a fix.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1611: Escape to Host	
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

CVE-2026-123007: https://my.f5.com/manage/s/article/K000163926

CVE-2026-123633: https://my.f5.com/manage/s/article/K000163928

CVE-2026-123634: https://my.f5.com/manage/s/article/K000163925

CVE-2026-121810: https://my.f5.com/manage/s/article/K000163927

CVE-2026-113425: https://my.f5.com/manage/s/article/K000163931

References

https://my.f5.com/manage/s/article/K000163926

https://nginx2root.com/

https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities

https://my.f5.com/manage/s/article/K000163928

https://my.f5.com/manage/s/article/K000163925

https://my.f5.com/manage/s/article/K000163927

https://my.f5.com/manage/s/article/K000163931

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 19, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com