NGINX HTTP/2 flaw CVE-2026-123007 allows unauthenticated code execution; patched versions released



A decade-old flaw in NGINX's HTTP/2 support, CVE-2026-123007 ("nginx2root"), can let an unauthenticated attacker run code on servers with HTTP/2 enabled. Fixed versions 1.31.9 and 1.30.7 are available.

- CVE-2026-123007, named "nginx2root", affects NGINX servers with HTTP/2 enabled.
- An attacker does not need to log in to run code.
- The flaw has existed in the open-source code since version 1.9.5, released on September 22, 2015.
- Fixed versions 1.31.9 and 1.30.7 have been released.
- F5, the company behind NGINX, describes the impact as code execution by attackers.

What was reported

A flaw in NGINX's HTTP/2 support can allow an attacker to execute code on a server without authenticating. The issue is tracked as CVE-2026-123007 and has been nicknamed "nginx2root". It affects servers on which HTTP/2 is enabled.

The weakness has been present in NGINX's open-source code since version 1.9.5, released on September 22, 2015, which means it went unnoticed for about ten years.

Fix status

NGINX versions 1.31.9 and 1.30.7 contain the fix and were released on the day of the report. F5, the company behind NGINX, states that attackers can use the flaw to run code. The source excerpt does not give further technical detail, such as exploitation status or workarounds, so teams should consult the F5 and NGINX advisories directly.

What this means for regulated institutions

NGINX is commonly used as a web server, reverse proxy or load balancer, often at the edge of the network and exposed to the internet. A flaw that needs no credentials and affects a widely enabled protocol deserves prompt attention. The first step is to know where NGINX runs, including inside appliances, containers and third-party products, and whether HTTP/2 is enabled on it.

Patching should follow your normal emergency change process, with the affected systems prioritised by exposure and business criticality.

What to do now

1. Inventory all NGINX instances, including those embedded in appliances, containers and vendor products.
2. Identify which instances have HTTP/2 enabled, starting with internet-facing ones.
3. Upgrade to NGINX 1.31.9 or 1.30.7, or apply the vendor's equivalent fix, through the emergency change process.
4. Ask third-party vendors whose products bundle NGINX for their patch status and timelines.
5. Review web server and proxy logs for unusual activity and record the vulnerability in your vulnerability management register.