F5 patches five critical NGINX flaws grouped as NGINX2Root



F5 has fixed five critical NGINX vulnerabilities that can allow remote code execution under certain conditions. No exploitation in the wild is reported, but a public proof-of-concept exists for one of them.

- Five critical NGINX flaws, named NGINX2Root by Xint, can allow remote code execution with the privileges of the worker process if ASLR is disabled or bypassed.
- CVE-2026-123007 has a public proof-of-concept; Rapid7 describes it as constrained, needing roughly 128 GB of HTTP/2 traffic and an ASLR bypass.
- No exploitation in the wild is reported, and none were in CISA's KEV catalog as of November 19.
- Reaching root requires a sixth flaw, an unpatched Linux kernel SCTP bug with no CVE as of November 18.

> - Fixed releases are NGINX Open Source 1.30.7 and 1.31.9, and NGINX Plus 37.0.8.1 and 37.3.0.1; a restart is required after upgrading.

F5 has released fixes for five critical vulnerabilities in NGINX, which Xint researchers named NGINX2Root. Under certain conditions they can allow remote code execution. Two of them, CVE-2026-123633 and CVE-2026-123007, were also reported independently by several other research teams.

What is affected

Three of the flaws are use-after-free issues tied to HTTP/2, the DNS resolver and HTTP/3 over QUIC, and a fourth sits in the mail proxy's auth_http path. The fifth, CVE-2026-123007, is an integer underflow in HTTP/2 flow control that can crash a worker process and potentially allow code execution. If ASLR is disabled or bypassed, any of the five can give code execution with the privileges of the NGINX worker process. Becoming root needs a sixth flaw in the Linux kernel's SCTP code, which had no CVE and no patch as of November 18.

Exploitation status

No exploitation in the wild is reported. A public proof-of-concept exists for CVE-2026-123007, which Rapid7 describes as constrained: it relies on an x86-64 glibc routine, needs about 128 GB of HTTP/2 traffic and must recover heap addresses to defeat ASLR. Tenable notes it is unlikely to work behind HTTP/2-terminating proxies or on slow connections. Xint and Wiz hold exploits for all five but have not published them.

Fixing it

Upgrading is preferable to mitigations. The fixed releases are NGINX Open Source 1.30.7 and 1.31.9, and NGINX Plus 37.0.8.1 and 37.3.0.1. NGINX must be restarted afterwards, as a configuration reload does not replace the running executable. Distribution package users should check for backported fixes. NGINX also ships inside other F5 products; some have updates and others are still being worked on.

What to do now

1. Inventory all NGINX instances, including those embedded in NGINX Instance Manager, Ingress Controller and Gateway Fabric, and prioritise internet-facing ones.
2. Upgrade to the fixed NGINX releases and restart the service; do not rely on a configuration reload.
3. For distribution packages, confirm with the vendor that the fixes have been backported.
4. Check that ASLR is enabled on hosts running NGINX and track the pending Linux kernel SCTP fix.
5. Review the Xint guidance for investigating possible CVE-2026-123007 activity on exposed servers.
6. Reduce internet-facing systems, automate patching and limit what each application can access.