CYBER THREAT INTELLIGENCE

CRITICALSTART® Security Advisory

TLP CLEAR // [CS-SA-26-1104] NGINX HTTP/2 Remote Code Execution Vulnerabilities

Executive Summary

The CRITICALSTART® Cyber Research Unit (CRU) is tracking two critical memory-safety flaws in the Hypertext Transfer Protocol version 2 (HTTP/2) implementation of NGINX, CVE-2026-123007 and CVE-2026-123633, each allowing unauthenticated remote code execution (RCE) as the NGINX worker process. CVE-2026-123007 affects every release since 2015, even on static-file servers.[1, 2] F5 released fixes on November 18, 2026, and a working public PoC for CVE-2026-123007 was published the same day.[2] Organizations should upgrade to NGINX 1.30.7 or 1.31.9 or fixed NGINX Plus builds and disable HTTP/2 where they cannot.

Overview

Between October 16 and November 16, 2026, Wiz Research, Ikotas Labs, Metnir, Rapid7, and Xint independently reported multiple vulnerabilities in NGINX to F5.[1, 3, 4, 5] The two most significant flaws, CVE-2026-123007 and CVE-2026-123633, can allow remote code execution (RCE) through memory corruption in NGINX worker processes. The disclosures involved coordinated research, with Wiz and Xint using AI-assisted code analysis. F5's security fixes credit Xint for CVE-2026-123007 and Albert of Vexera AI for CVE-2026-123633, while Rapid7 researcher Stephen Fewer independently identified CVE-2026-123007.[3, 4] The same release addresses three additional RCE vulnerabilities: CVE-2026-123634, CVE-2026-121810, and CVE-2026-113425. Xint also reported a separate, unpatched Linux kernel vulnerability involving Stream Control Transmission Protocol (SCTP), which could allow an attacker to escalate NGINX worker privileges to root, including from within a container. No exploitation in the wild or threat actor attribution has been reported. However, Xint identified approximately 56.7 million NGINX hosts through Shodan, with 98.9% reportedly running versions within the affected range for CVE-2026-123007.[5]

Technical Details

CVE-2026-123007 - HTTP/2 Flow-Control Integer Underflow: The vulnerability occurs when a client cancels an HTTP/2 stream while response data remains queued for transmission. NGINX incorrectly restores the queued data to the connection's send-window counter without enforcing the protocol's maximum permitted value. A subsequent `WINDOW_UPDATE` frame can exploit an unsigned integer bounds-check error, causing the counter to wrap and accept an invalid increase. The resulting oversized value can produce a negative length during a memory operation in the TLS transmission path, triggering an out-of-bounds copy that allows attackers to disclose and overwrite NGINX worker memory.[2]

CVE-2026-123633 - HTTP/2 Use-After-Free: This vulnerability involves improper connection lifecycle management during HTTP/2 request processing. When NGINX receives a partially transmitted HEADERS frame, it can incorrectly mark the associated connection as reusable even though request processing has begun. If the worker subsequently exhausts its available connection slots while establishing an upstream connection, it may release the client connection prematurely. Continued processing then accesses the freed memory, resulting in a use-after-free condition. Exploitation requires NGINX to proxy requests to a backend server.[1, 4]

© 2026 Critical Start. All rights reserved.

From Memory Corruption to Remote Code Execution: Both vulnerabilities provide opportunities for attackers to disclose and manipulate worker memory. The resulting memory disclosure can help overcome Address Space Layout Randomization (ASLR), making it easier to identify memory locations needed for exploitation. Wiz and Rapid7 independently demonstrated remote code execution against official NGINX builds, confirming that the vulnerabilities can extend beyond denial of service or information disclosure.[1, 2]

Exploitation Constraints: The publicly demonstrated exploit for CVE-2026-123007 requires approximately 128 GB of HTTP/2 traffic over a single connection. At bandwidths below approximately 300 Mbps, the transfer may exceed NGINX's default one-hour connection lifetime, limiting practical exploitation. The demonstrated technique also depends on a specific glibc `memcpy` implementation used on x86-64 processors supporting AVX-512. Additionally, content delivery networks (CDNs) that reframe HTTP/2 traffic may disrupt the exploit's required conditions.[2]

MITRE ATT&CK Mapping

The following MITRE ATT&CK mapping summarizes the techniques relevant to the reported NGINX vulnerabilities:

ID	Name	Relevance
T1190	Exploit Public-Facing Application	Unauthenticated HTTP/2 traffic to an internet-facing NGINX listener
T1059.004	Command and Scripting Interpreter: Unix Shell	Public PoC redirects a callback to system() to run attacker commands
T1068	Exploitation for Privilege Escalation	Xint chains worker access with the unpatched kernel SCTP flaw to reach host root, including from a container

Relevant Vulnerability Context

HTTP/2 is off by default in NGINX, but most HTTPS deployments enable it, and the lower nginx.org rating for CVE-2026-123633 reflects its narrower trigger.[4]

CVE	CVSS	Description	Relevance
CVE-2026-123007	4.0: 9.2 (F5, Rapid7) 3.1: 8.1 (F5)	Integer underflow in HTTP/2 flow control (CWE-191) leading to an out-of-bounds write (CWE-787)	Any HTTP/2 configuration, including static file serving; public PoC
CVE-2026-123633	4.0: 9.2 (F5) 3.1: 8.1 (F5)	Use-after-free in HTTP/2 connection reuse (CWE-416)	HTTP/2 plus proxying to an upstream under connection pressure

Implications for Organizations

Exposure is potentially widespread, as a large proportion of internet-facing NGINX deployments may be affected by CVE-2026-123007. Although the demonstrated exploit currently requires substantial traffic and specific system configurations, CRU assesses with moderate confidence that further exploit development will reduce these constraints and make attacks more practical. The availability of public proof-of-concept code and multiple independent vulnerability discoveries increases the likelihood of continued exploitation research.

© 2026 Critical Start. All rights reserved.

Packaged NGINX deployments, including internet-facing appliances, ingress controllers, and container images, warrant particular attention because widely distributed builds could expose multiple organizations to the same attack techniques. Successful worker-process compromise could also expose sensitive information handled by proxied applications, including session cookies, authentication tokens, and API keys. Organizations should therefore consider potential credential exposure when investigating suspected exploitation. Disabling HTTP/2 may reduce exposure to certain attack paths, but it does not address the three additional RCE vulnerabilities included in the same security release. Furthermore, version strings alone may not reliably establish patch status when vendors backport security fixes. Organizations should verify vendor-specific patch status and prioritize deploying the complete security updates across all affected NGINX instances.

Prioritized Mitigation Strategies

To reduce exposure to CVE-2026-123007 and CVE-2026-123633 and limit the risk of remote code execution through NGINX, CRU recommends the following actions:

Immediate (Within 24 Hours)

- Identify affected NGINX deployments. Inventory all NGINX Open Source and NGINX Plus instances, prioritizing internet-facing servers. Identify deployments with HTTP/2 enabled and determine which configurations proxy requests to upstream servers, as these conditions affect exposure to the two HTTP/2 vulnerabilities.[1, 2]
- Upgrade affected NGINX instances. Install NGINX Open Source 1.30.7 or 1.31.9, or NGINX Plus 37.0.8.1 or 37.3.0.1. These releases address the two HTTP/2 vulnerabilities. Follow the applicable F5 advisory for branch-specific upgrade requirements. Restart NGINX after upgrading to ensure the running worker processes use the patched binary.[1, 2]
- Temporarily disable HTTP/2 if immediate patching is not possible. On NGINX 1.25.1 and later, configure http2 off; in affected server blocks and remove the http2 parameter from applicable listen directives. Test application compatibility, reload NGINX, and confirm that existing worker processes have exited. Re-enable HTTP/2 only after installing the fixes.[2]

Short-Term (Within Two Weeks)

- Verify distribution and container builds. Check package versions against vendor advisories, not `nginx -v`, and rebuild pinned container images.
- Verify vendor and distribution-specific updates. Check package versions against the relevant vendor security advisories rather than relying exclusively on nginx -v, as distributions may backport security fixes. Include NGINX embedded in third-party appliances, container images, and other packaged applications.
- Rebuild and redeploy container images. Update pinned NGINX base images to patched release sand rebuild affected workloads. Verify that running containers use the corrected images rather than assuming that updating the image in a registry also updates deployed instances.
- Address the additional vulnerabilities. Review exposure to CVE-2026-123634, CVE-2026-121810,and CVE-2026-113425. These affect specific configurations involving the DNS resolver and mirror module, HTTP/3 (QUIC), and mail proxy authentication, respectively. Apply the corresponding security updates and review the affected features where upgrades are delayed.[3, 4]

Structural

- Maintain visibility into NGINX deployments. Track NGINX versions, enabled modules, and relevant configurations across servers, appliances, and container environments. Include embedded NGINX components in Software Bills of Materials (SBOMs) to improve vulnerability identification and patch tracking.

© 2026 Critical Start. All rights reserved.

- Strengthen post-exploitation monitoring. Monitor for unexpected NGINX worker crashes, segmentation faults, unusual child processes, and unexpected command execution originating from NGINX workers. Investigate suspicious activity alongside application and system logs, as these behaviors may indicate attempted exploitation but are not definitive indicators of compromise.[1, 2]

Conclusion

These flaws make NGINX, the internet's most common front door, an unauthenticated entry point past every application behind it. Near-term risk sits with directly exposed servers and packaged builds, and the exploit's bandwidth demands buy only temporary relief. Organizations that upgraded, verified the real package, and restarted NGINX are protected against all five flaws; those relying on disabled HTTP/2 or version strings are not. As AI-assisted discovery surfaces old memory bugs in core web infrastructure, edge patch cycles must keep shortening.

For more threat reports, including OPTIMJACK, ARTEX, and Java4Shell, visit Critical Start's Intel Hub. This advisory was written using the best intelligence available at the time and is subject to change as additional information becomes available.

What Critical Start is Doing

The CRITICALSTART® Cyber Research Unit (CRU) will continue to work closely with the SOC and Security Engineering team to implement any relevant detections and increase vigilance. Critical Start customers are encouraged to reach out to support@criticalstart.com for any further enquiries.

Further Reading

[1] Wiz Research (November 18, 2026). Unauthenticated Remote Code Execution in NGINX: CVE-2026-123633 and CVE-2026-123007. https://www.wiz.io/blog/nginx-http2-rce-vulnerabilities

[2] Rapid7 (November 18, 2026). CVE-2026-123007: Critical NGINX HTTP/2 Integer Underflow Leads to RCE (FIXED). https://www.rapid7.com/blog/post/ve-cve-2026-123007-critical-nginx-http-2-integer-underflow-leads-to-rce-fixed/

[3] F5, Inc. (November 18, 2026). Security Advisories K000163926 (CVE-2026-123007) and K000163928 (CVE-2026-123633). https://my.f5.com/manage/s/article/K000163926

[4] JFrog Security Research (November 18, 2026). Nginx2Shell: All You Need to Know About CVE-2026-123007 and CVE-2026-123633. https://research.jfrog.com/post/nginx2shell-all-you-need-to-know-about-cve-2026-123007-and-cve-2026-123633/

[5] Equixly (November 18, 2026). nginx2root: Disabling HTTP/2 Stops Two of Five nginx RCE Flaws. https://equixly.com/blog/2026/11/18/nginx2root-disabling-http-2-stops-two-of-five-nginx-rce-flaws/

[6] Cyber Security News (November 18, 2026). NGINX HTTP/2 Flaws Could Allow Memory Corruption and Remote Code Execution on Web Servers. https://cybersecuritynews.com/nginx-http-2-vulnerabilities/

© 2026 Critical Start. All rights reserved.

Appendices

Appendix A: Affected and Fixed Builds

Product	CVE	Affected	First Fixed
NGINX Open Source	CVE-2026-123007	1.9.5 to 1.30.6; 1.31.0 to 1.31.8	1.30.7 (stable); 1.31.9 (mainline)
NGINX Open Source	CVE-2026-123633	1.19.7 to 1.30.6; 1.31.0 to 1.31.8	1.30.7 (stable); 1.31.9 (mainline)
NGINX Plus 37.x	CVE-2026-123007	37.0.0 to 37.0.7.1; 37.1.0 to 37.2.0.1	37.0.8.1; 37.3.0.1
NGINX Plus 37.x	CVE-2026-123633	37.0.0 to 37.0.6.1; 37.1.0 to 37.2.0	37.0.7.1; 37.2.0.1
NGINX Plus R-series	Both	R33 to R36	No fix listed; move to 37.0.8.1 or 37.3.0.1
Official NGINX container images	Both	Images built on 1.31.8 or earlier	Rebuild on 1.30.7 or 1.31.9 images when published
kubernetes/ingress-nginx	Both	All releases (project archived)	No fix planned; migrate
Products embedding NGINX	Both	Depends on bundled build	Vendor-specific fixed build

Appendix B: Detection and Hunting

Indicator	What to Look For
Worker process execution	Shell or utility (`sh`, `bash`, `curl`, `wget`, `python`) with an NGINX worker as parent
Worker crashes	Repeated `exited on signal 11` (or signal 6) in the error log, often from one source
Flow-control abuse	Single HTTP/2 session lasting minutes with tens of GB inbound while logged request sizes stay small
Connection churn	Many short TLS connections from one source alongside crashes
Kernel escalation prep	`sctp` module loaded on a web host that does not use SCTP

Note: `WINDOW_UPDATE` and `RST_STREAM` frames do not appear in access logs. No confirmed indicators of compromise have been published as of November 18, 2026. [2], [4], [5]

Exposure checks

Run the following on each NGINX host or container):

```
nginx -v
nginx -V 2>&1 | grep -c http_v2_module        # 0 means no HTTP/2 code in the binary
nginx -T 2>/dev/null | grep -nE '^\s*(http2\s+on\b|listen\b[^#]*\bhttp2\b)'
```

© 2026 Critical Start. All rights reserved.

```
nginx -T 2>/dev/null | grep -nE '\b(proxy|fastcgi|uwsgi|scgi|grpc)_pass\b'
openssl s_client -connect HOST:443 -servername HOST -alpn h2 </dev/null | grep ALPN
```

Any HTTP/2 output on an unpatched build indicates exposure to CVE-2026-123007; proxy output adds CVE-2026-123633. Behind a CDN, test the NGINX origin directly.[4, 5]

Hunting commands:

```
grep "exited on signal" /var/log/nginx/error.log
docker logs <container> 2>&1 | grep "exited on signal"
auditctl -a always,exit -F arch=b64 -S execve -F uid=$(id -u www-data) -k nginx_exec
lsmod | grep -w sctp
```

© 2026 Critical Start. All rights reserved.