ÖFFENTLICHER POC · LAUT CERT-FR

THREAT INTELLIGENCE BRIEFING

CVE-2026-123007

Speicherkorruption in der HTTP/2-Flusssteuerung von NGINX.

Ein nicht authentifizierter Angreifer aus dem Netz kann über HTTP/2 einen Heap-Überlauf im NGINX-Worker auslösen. Meist führt das zum Absturz des Prozesses. Wiz hat auf offiziellen Builds Codeausführung mit ASLR-Umgehung bestätigt; laut CERT-FR ist ein öffentlicher PoC bekannt. Eine Ausnutzung in freier Wildbahn ist nicht bekannt.

Geschäftsrisiko: Dienstausfall von Web- und Reverse-Proxy-Diensten, im Extremfall die Übernahme des Servers – mit Potenzial für Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,2 / 10

KRITISCH
CVSS 4.0 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` – aus dem Netz, ohne Rechte, ohne Zutun, bei hoher Angriffskomplexität, mit voller Wirkung auf den betroffenen Dienst. Von F5 als CNA vergeben, laut NVD. CVSS 3.1 Basiswert 8,1.

AUSNUTZUNG
Nicht bekannt (Stand 19.11.2026)

BETROFFEN
NGINX Open Source 1.9.5 bis 1.31.8 + NGINX Plus mit eingeschaltetem HTTP/2

HANDLUNGSBEDARF
Sofort – HTTP/2 abschalten, dann patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,2 · KRITISCH
CVSS-Schweregrad

HTTP/2
Voraussetzung: HTTP/2 ist eingeschaltet

Nicht bekannt
Ausnutzung · nicht in CISA KEV · PoC öffentlich laut CERT-FR

1.31.9 · 1.30.7
Fixversionen NGINX Open Source seit 18.11.2026

Die Ursache: Die HTTP/2-Flusssteuerung lässt das Flow-Control-Window über den zulässigen Wert hinaus wachsen (Integer-Unterlauf, CWE-191); die Folge ist ein Heap-Pufferüberlauf (CWE-787). Laut F5 stürzt der Worker typischerweise ab; bei abgeschaltetem oder umgangenem ASLR ist Codeausführung möglich. Wiz hat Codeausführung mit ASLR-Umgehung auf offiziellen Builds 1.31.7 und 1.31.8 bestätigt – auf einem Server mit nur statischen Dateien. Eingeschleuster Code läuft mit den Rechten des Worker-Prozesses; Rapid7 nennt für seinen Angriffsweg rund 128 GB HTTP/2-Verkehr, was Angriffe über das Internet praktisch bremst. nginx.org dankt Xint.io für den Fund.

ANGRIFFSKETTE

01 **HTTP/2 erreichbar** – NGINX nimmt HTTP/2-Verbindungen direkt aus dem Netz an

02 **Fenster verfälschen** – der Integer-Unterlauf erzeugt ein ungültiges Flow-Control-Window

03 **Speicher überschreiben** – Heap-Überlauf; laut Rapid7 fließen Heap- und Bibliothekszeiger ab

04 **Absturz oder Übernahme** – Worker-Absturz; mit ASLR-Umgehung führt ein umgelenkter Cleanup-Callback Befehle aus (Rapid7)

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
NGINX Open Source	`1.9.5 bis 1.31.8`	`1.31.9 · 1.30.7`
NGINX Plus 37	`37.0.x vor 37.0.8.1 · 37.1–37.3 vor 37.3.0.1`	`37.0.8.1 · 37.3.0.1`
Plus R33–R36, F5-Produkte, Red Hat	betroffen laut F5 bzw. NVD	im Hersteller-Advisory prüfen

Backports zeigt `nginx -v` nicht – maßgeblich ist die volle Paketversion. Ubuntu: behoben in `1.24.0-2ubuntu7.20` (24.04) und `1.18.0-6ubuntu14.23` (22.04). Gleiche Notlösung wie bei `CVE-2026-123633`.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

18.11.2026
F5-Advisory · Fix 1.31.9 / 1.30.7

18.11.2026
CERT-FR-Warnung ALE-017

Stand heute
PoC öffentlich laut CERT-FR

Stand heute
Keine Ausnutzung bekannt

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Notlösung vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
HTTP/2 abschalten	NGINX auf 1.31.9 oder 1.30.7 patchen	Worker-Abstürze in den Logs prüfen

01 Betroffenheit feststellen

Alle NGINX-Instanzen erfassen; Voraussetzung ist eingeschaltetes HTTP/2. Erscheint `ALPN protocol: h2`, nimmt der Server HTTP/2 an; keine Ausgabe heißt nur dann „aus“, wenn die Seite per HTTPS normal lädt. Hinter CDN oder Load Balancer direkt gegen NGINX testen; HTTP/2 ohne TLS erfasst der Test nicht (dazu `nginx -T` nach `http2` durchsuchen).

```
openssl s_client -connect HOST:443 -
servername HOST -alpn h2 </dev/null 2>&1
| grep -F 'ALPN protocol: h2'
```

02 Sofort mitigieren (vor dem Patch)

Ab NGINX 1.25.1 in allen server-Blöcken `http2 off;` setzen bzw. `http2 on;` entfernen und den Parameter `http2` aus allen `listen`-Zeilen streichen. Bis 1.25.0 gibt es die Direktive nicht: dort nur den Parameter entfernen (`listen 443 ssl http2;` → `listen 443 ssl;`). Offene HTTP/2-Verbindungen bleiben nach dem Reload bei den alten Workern – laufen noch Prozesse „worker process is shutting down“, NGINX neu starten. Dienste, die HTTP/2 brauchen (z. B. natives gRPC), sind betroffen.

```
sudo nginx -t && sudo nginx -s reload
```

03 Patchen

Auf NGINX `1.31.9` (Mainline) bzw. `1.30.7` (Stable) aktualisieren, NGINX Plus auf `37.0.8.1` bzw. `37.3.0.1`, Distributionspakete laut Sicherheitshinweis; das Release behebt zugleich weitere NGINX-Lücken. Danach NGINX neu starten – ein Reload tauscht das Programm nicht aus – und HTTP/2 bei Bedarf wieder einschalten. Container-Images, Ingress-Controller und F5-Produkte mit eingebautem NGINX gesondert auf den Herstellerstand bringen.

04 Kompromittierung ausschließen

Error-Logs auf Worker-Abstürze (`worker process … exited on signal 11`) und häufige Neustarts prüfen. Zugriffslogs zeigen den Angriff kaum; aussagekräftiger sind vom Worker gestartete Programme (z. B. `/bin/sh`) und die Verbindungsstatistik. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – es ist keine Ausnutzung in freier Wildbahn bekannt

ERKENNUNGSHINWEISE

`worker process … exited on signal 11` im error.log

auffällig häufige Worker-Neustarts

AUFFÄLLIGE MUSTER

unerwartete Kindprozesse oder ausgehende Verbindungen des Workers

minutenlang offene Verbindung einer externen IP mit stark wachsendem Datenvolumen (`ss -tinp`)

Zur Einordnung: Keine CVE-spezifischen Indikatoren bekannt; die Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: Ein Absturz sieht zunächst wie ein gewöhnlicher Dienstfehler aus. Ohne Auswertung der Error-Logs und der Neustart-Muster bleibt ein Missbrauch oft unbemerkt.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Im Cyber Defense Center fallen wiederkehrende Worker-Abstürze am NGINX-Dienst in der Log-Auswertung auf – sofern die Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare NGINX-Server mit eingeschaltetem HTTP/2 über Ihren gesamten Perimeter und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre NGINX-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Auswertung der Erkennungshinweise, danach laufendes Monitoring und IR-Bereitschaft, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Notlösung HTTP/2 heute anordnen, Update zeitnah einplanen.
- Prüfen lassen, welche NGINX-Systeme inklusive Container, NGINX Plus und Distributionspakete HTTP/2 eingeschaltet haben.
- Über eine dauerhafte Überwachung der Reverse-Proxy-Systeme entscheiden.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-123007 und dem NGINX-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: F5-Advisory K000163926 (18.11.2026; die F5-Seite ist ohne JavaScript nicht maschinell lesbar, Versionsangaben daher aus nginx.org und NVD) · nginx.org CHANGES (1.31.9, 1.30.7) · NVD (CVE-2026-123007, Status „Analyzed“; CVSS 4.0 9,2, CVSS 3.1 8,1) · CERT-FR CERTFR-2026-ALE-017 und CERTFR-2026-AVI-1567 (18.11.2026) · CISA KEV (Katalogstand 18.11.2026: nicht gelistet; SSVC-Einstufung) · Wiz und Rapid7 (ASLR-Umgehung) · Xint (Entdeckung) · Ubuntu-Sicherheitshinweise. Stand 19.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.

Bildmotive: KI-generierte Symbolbilder