THREAT INTELLIGENCE BRIEFING

CVE-2026-123633

Use-after-free in HTTP/2 bei NGINX im Reverse-Proxy-Betrieb.

Ein Speicherfehler im NGINX-Worker (Use-after-free) kann im Reverse-Proxy-Betrieb mit HTTP/2 zum Dienstausfall führen. Laut F5 ist bei abgeschaltetem oder umgangenem ASLR auch Codeausführung möglich; Wiz hat die Lücke an F5 gemeldet und Codeausführung mit ASLR-Umgehung bestätigt. Ein öffentlicher PoC für diese Lücke ist nicht bekannt. Xint hat den Angriffsweg technisch beschrieben, die letzten Schritte aber bewusst weggelassen.

> **Geschäftsrisiko:** Ausfall des Reverse Proxys und der dahinterliegenden Anwendungen, 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 1.19.7 bis 1.31.8 im Reverse-Proxy-Betrieb mit HTTP/2

HANDLUNGSBEDARF
Dringend – Notlösung heute, Patch zeitnah

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,2 · KRITISCH
CVSS-Schweregrad

Reverse Proxy
Voraussetzungen: HTTP/2 und Weiterleitung an ein Backend

Nicht bekannt
Ausnutzung · kein öffentlicher PoC · nicht in CISA KEV

1.31.9 · 1.30.7
Fixversionen NGINX Open Source seit 18.11.2026

Die Ursache: Der NGINX-Worker greift bei HTTP/2 auf bereits freigegebenen Speicher zu (**CWE-416, Use-after-free**). Voraussetzung sind HTTP/2 für Client-Verbindungen, die Weiterleitung an ein Backend und knappe `worker_connections`. Folge ist ein Absturz (Denial of Service); laut F5 ist bei abgeschaltetem oder umgangenem ASLR auch Codeausführung möglich. nginx.org dankt Albert of Vexera AI; Wiz meldete die Lücke ebenfalls an F5 – laut Wiz hatte ein anderes Team sie zuvor gemeldet.

ANGRIFFSKETTE

01 **HTTP/2 als Reverse Proxy** – NGINX nimmt HTTP/2 an und reicht Anfragen an ein Backend weiter

02 **Verbindungen verknappen** – offene HTTP/2-Anfragen binden die `worker_connections`; NGINX räumt eine noch genutzte Verbindung ab (Wiz, Xint)

03 **Speicher falsch verwenden** – der Worker greift auf bereits freigegebenen Speicher zu

04 **Absturz oder Codeausführung** – Denial of Service; bei umgangenem ASLR laut F5 Codeausführung

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
NGINX Open Source	`1.19.7 bis 1.31.8`	`1.31.9 · 1.30.7`
NGINX Plus 37	`37.0.x vor 37.0.7.1 · 37.1–37.2 vor 37.2.0.1`	`37.0.7.1 · 37.2.0.1`
Plus R33–R36, F5-Produkte, Red Hat	betroffen laut F5 bzw. NVD	im Hersteller-Advisory prüfen

Ubuntu stuft auch 22.04 (`1.18.0`) als betroffen ein – dort nur bei HTTP/2-Listenern ohne TLS – und behebt die Lücke mit `1.18.0-6ubuntu14.23` (24.04: `1.24.0-2ubuntu7.20`). Gleiche Notlösung und gleiches Release wie `CVE-2026-123007` – beide Lücken gemeinsam schließen.

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

19.11.2026
NVD-Status „Analyzed“

Stand heute
Kein PoC · nicht in CISA KEV

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

Prüfen, ob NGINX als Reverse Proxy HTTP/2 für Client-Verbindungen nutzt und an Backends weiterreicht – nur diese Kombination ist betroffen. 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` (für diese Lücke allein reichen laut NVD `37.0.7.1` bzw. `37.2.0.1`), Distributionspakete laut Sicherheitshinweis. 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; Verbindungen von NGINX zu den Backends auf ungewöhnliche Muster ansehen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – kein öffentlicher PoC bekannt

ERKENNUNGSHINWEISE

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

häufige Worker-Neustarts unter Last

AUFFÄLLIGE MUSTER

ungewöhnlich viele offene Verbindungen eines Workers

ausgehende Verbindungen des Workers zu unbekannten Adressen

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

Wichtig: Die Lücke greift bei gezielt aufgebauten Verbindungen, begünstigt durch hohe Last. Ein Absturz sieht dann wie ein gewöhnlicher Dienstfehler aus; ohne Auswertung der Error-Logs bleibt die Ursache oft unerkannt.

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 Reverse Proxy in der Log-Auswertung auf – sofern die Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden öffentlich erreichbare NGINX-Reverse-Proxys mit 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 oder Update für alle Reverse Proxys mit HTTP/2 priorisiert anordnen.
- Prüfen lassen, welche NGINX-Systeme im Reverse-Proxy-Betrieb HTTP/2 nutzen.
- Über eine dauerhafte Überwachung der Reverse-Proxy-Logs 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-2026-123633 und dem NGINX-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: F5-Advisory K000163928 (18.11.2026; die F5-Seite ist ohne JavaScript nicht maschinell lesbar, Angaben aus nginx.org und NVD) · nginx.org CHANGES (1.31.9, 1.30.7) und Security Advisories (Einstufung „medium“) · NVD (CVE-2026-123633, Status „Analyzed“) · CERT-FR CERTFR-2026-ALE-017 (18.11.2026) · CISA KEV (Katalogstand 18.11.2026: nicht gelistet) · Wiz (Meldung an F5, Codeausführung mit ASLR-Umgehung bestätigt) · Albert of Vexera AI (Entdeckung) · Ubuntu-Sicherheitshinweise. Stand 19.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.