DEFION

SECURITY ADVISORY
19 NOVEMBER 2026

Kritieke kwetsbaarheid in nginx (nginx2root)

Door een fout in de HTTP/2-afhandeling kan een aanvaller een nginx-server op afstand en zonder inloggegevens aanvallen. De patch is er sinds 18 november.

ERNST	KENMERK	STATUS
Kritiek (CVSS 4.0: 9,2)	CVE-2026-123007	Patch beschikbaar Publieke proof of concept

01 · KERNBOODSCHAP

In nginx zit een kritieke kwetsbaarheid waarmee een aanvaller op afstand en zonder inloggegevens het servergeheugen kan corrumperen en volgens de ontdekkers code kan uitvoeren. Voor Debian en Red Hat is er nog geen hersteld pakket.

ONS ADVIES IN VIER PUNTEN

Werk vandaag bij. Kan dat nog niet, zet HTTP/2 dan uit tot uw distributie de fix uitbrengt.

01 Bepaal de volgorde
Begin met nginx-servers die vanaf internet bereikbaar zijn en HTTP/2 gebruiken, ook in Kubernetes en appliances.

02 Zet HTTP/2 uit
Zet http2 off; en verwijder http2 uit elke listen op de poort. Herlaad en controleer dat h2 niet meer wordt aangeboden.

03 Werk bij en herstart
nginx 1.30.7 of 1.31.9, of het herstelde pakket van uw distributie. Een reload vervangt de binary niet.

04 Blokkeer SCTP
Doe dit op hosts die SCTP niet gebruiken. Voor de kernelfout is nog geen patch.

Weet u niet welke versie een nginx draait, behandel die server dan als kwetsbaar.

02 · WAT SPEELT ER

Kwetsbaar zodra HTTP/2 aanstaat

- Het gaat om **CVE-2026-123007**. Het bedrijf Xint noemt de fout “nginx2root” en beschrijft daarbij ook een nog niet gepatchte fout in de Linux-kernel, waarmee een aanvaller vanuit nginx root-rechten krijgt. Vier andere fouten in nginx staan hier los van.
- Ernst: kritiek. F5 geeft een 9,2 onder CVSS 4.0 en een 8,1 onder CVSS 3.1. Om code uit te voeren moet een aanvaller ASLR omzeilen. De onderzoekers beschrijven hoe dat kan.
- Kwetsbaar zijn nginx 1.9.5 tot en met 1.31.8 en NGINX Plus, ook in distributiepakketten, containerimages, Kubernetes-ingresscontrollers en afgeleiden als OpenResty en Tengine.
- Voorwaarde: HTTP/2 staat aan en is bereikbaar. Dat is geen standaardinstelling, dus controleer elke server.
- Met alleen deze kwetsbaarheid kan een aanvaller workerprocessen laten crashen of, met de volledige exploit, code uitvoeren. Hij kan dan bij de TLS-sleutels, het verkeer door de proxy en de inloggegevens voor de backends. Combineert hij dit met de kernelfout, dan krijgt hij root-rechten op de host, ook vanuit een Docker-container.
- Er is geen misbruik bekend. De exploit van Rapid7 werkt alleen onder gecontroleerde omstandigheden, maar bewijst dat de fout te misbruiken is.

03 · WAAR ZIT NGINX

Op meer plekken dan u denkt

Controleer ook nginx in producten en diensten van derden.

Eigen servers en proxy's

Websites, API's en loadbalancers.

Kubernetes

Bij ingress-nginx staat HTTP/2 aan. Het project is gearchiveerd en krijgt geen patch (Upwind).

Containers en afgeleiden

Docker-images, OpenResty, Tengine en Angie.

Systemen van derden

Appliances en beheerde diensten waarin nginx is verwerkt.

> De vier andere nginx2root-kwetsbaarheden staan los van deze fout. Ze zijn alleen te misbruiken bij een specifieke configuratie: HTTP/3, een resolver met mirror of SSI, of de mailproxy. Zie sectie 06.

04 · STAPPENPLAN

Wat u nu doet

Voer stap 1 tot en met 4 vandaag uit. Stap 5 tot en met 7 volgen binnen 72 uur.

Vandaag

Inventariseren en afschermen

01 Inventariseer waar nginx draait

Draai `nginx -v`. Vergelijk bij distributiepakketten de pakketversie (`dpkg -l 'nginx*'` of `rpm -q nginx`) met de advisory van uw distributie.

02 Controleer of HTTP/2 aanstaat

Op de server:

```
sudo nginx -T 2>&1 | sed 's/#.*//' | grep -nE 'listen[[:space:]].*http2|^[[:space:]]
*http2[[:space:]]+on[[:space:]]*;'
```

Van buiten uw netwerk:

```
openssl s_client -connect HOST:443 -servername HOST -alpn h2 </dev/null 2>&1 | grep
-E 'ALPN protocol|No ALPN'
```

- `h2` betekent blootgesteld. Geen uitvoer betekent dat de verbinding mislukte.
- Achter een CDN: herhaal de test tegen de origin.

03 Werk bij of zet HTTP/2 uit

Gebruikt u pakketten van nginx.org, de officiële Docker-image of Ubuntu, werk dan nu bij. Zet anders HTTP/2 uit.

- Vanaf 1.25.1: `http2 off;` en verwijder `http2` uit elke `listen` op de poort. Oudere versies: verwijder `http2` uit `listen`.
- Herlaad de configuratie. Herstart nginx als workers in de status “shutting down” blijven staan.
- ingress-nginx: `use-http2: "false"`.

> Let op: zonder HTTP/2 werkt native gRPC niet meer.

04 Kan HTTP/2 niet uit, scherm de server dan af

Beperk de toegang op IP-adres of plaats de server achter een CDN of laag-7-loadbalancer, zonder directe toegang tot de origin. Dat verkleint het risico, maar neemt het niet weg.

Binnen 72 uur

Patchen en controleren

05 Werk bij en herstart

Installeer de herstelde versie en herstart. Een reload is niet genoeg. Zet HTTP/2 pas daarna weer aan.

PRODUCT	STATUS OP 19 NOVEMBER 2026
nginx Open Source	Hersteld in 1.30.7 (stable) en 1.31.9 (mainline). Pakketten van nginx.org en de officiële Docker-image zijn beschikbaar.
NGINX Plus	Hersteld in 37.3.0.1 en 37.0.8.1. R33 tot en met R36 krijgen geen fix.
Debian, Ubuntu, RHEL	Ubuntu is hersteld (USN-9159-1). Debian 12 en 13 en RHEL 8 tot en met 10 zijn kwetsbaar en hebben nog geen hersteld pakket.
Kubernetes	NGINX Ingress Controller 5.8.0 en Gateway Fabric 2.9.0 zijn hersteld. ingress-nginx krijgt geen patch. Stap over op een alternatief.

06 Blokkeer SCTP

Controleer met `lsmod | grep sctp` dat SCTP niet in gebruik is. Zet daarna op de host, niet in de container, `install sctp /bin/false` in `/etc/modprobe.d/`.

- Een module die al geladen is, blijft actief. De regel werkt ook niet als SCTP in de kernel is ingebouwd.

07 Controleer op misbruik

- Een TLS-verbinding met tientallen GB inkomend en bijna niets uitgaand. Dit staat niet in het access log.
- Crashes van workers (`signal 11` in `error.log`).
- Elk proces dat door een nginx-worker is gestart. Dit is het duidelijkste teken van geslaagd misbruik.
- Vindt u sporen, isoleer en onderzoek dan de hele host, want de aanvaller kan root-rechten hebben. Vervang ook de TLS-certificaten en de inloggegevens voor de backends.

Doorlopend

Verhoogde waakzaamheid

- Laat uw SOC of MDR deze signalen volgen tot elke nginx is bijgewerkt.
- Blijf de komende dagen alert. Volgens VulnCheck werd de vorige ernstige nginx-fout (CVE-2026-42945) enkele dagen na de patch misbruikt.

05 · VEELGESTELDE VRAGEN

Als u doorvraagt

Is een reload genoeg?

Nee. Een nieuwe configuratie geldt alleen voor nieuwe verbindingen. Voor de patch is een herstart of een binary-upgrade (`USR2`) nodig.

Wij draaien Debian of Red Hat. Wat nu?

Er is nog geen hersteld pakket. Zet HTTP/2 uit tot uw distributie de fix uitbrengt.

Worden wij al aangevallen?

Er is geen misbruik bekend. De publieke exploit werkt alleen onder gecontroleerde omstandigheden en heeft ongeveer 128 GB verkeer nodig. Xint en Wiz hebben exploits die zij niet hebben gepubliceerd.

Wat kan DEFION doen?

Wij zoeken naar sporen van misbruik (MDR) en doen forensisch onderzoek als wij die vinden (DFIR). Ook testen wij of uw WAF, EDR of SIEM de publieke trigger detecteert (ITE).

De techniek in het kort

Integer overflow in de HTTP/2-flowcontrol van nginx (`ngx_http_v2_module`). Bij het annuleren van een stream geeft `ngx_http_v2_filter_cleanup()` krediet terug aan `send_window` zonder het maximum te controleren. Daardoor loopt de waarde van het venster over en wordt `memcpy()` in het TLS-pad met een enorme lengte aangeroepen. Het gevolg is een adreslek en een out-of-bounds write.

- Er is geen korte trigger. Na ongeveer 52 GiB aan WINDOW_UPDATE-frames op één TLS-verbinding wordt het venster negatief. Na ongeveer 60 GB crasht een worker en voor code-uitvoering is ongeveer 128 GB nodig. Aan dat volume is een aanval het best te herkennen.
- Voor detectie draait u `sudo ss -tinp state established '( sport = :443 )'` twee keer en vergelijkt u `bytes_received`. Log met auditd elke `execve` door de nginx-gebruiker.

OVERIGE CVE'S	VOORWAARDE	HTTP/2 UIT HELPT	MAATREGEL
CVE-2026-123633	HTTP/2, proxy naar een backend en bijna geen vrije verbindingen	Ja	Zet HTTP/2 uit.
CVE-2026-123634	`resolver`, `proxy_pass` met een variabele, mirror of SSI	Nee	`proxy_pass` naar een vaste `upstream`-groep.
CVE-2026-121810	HTTP/3, proxy naar een backend	Nee	Verwijder `listen … quic`, zet `http3 off;` en Alt-Svc 'clear'.
CVE-2026-113425	mail, `proxy on`, `auth_http`	Nee	Luister alleen op loopback of filter op IP-adres.

Bronnen: nginx.org/en/security_advisories.html · F5 K000163926 · Xint, xint.io/blog/nginx2root-remote-code-execution · Rapid7 · Upwind · VulnCheck

CONTACT

+31 88 733 13 37

Vragen of hulp nodig? Neem contact op met uw directe contactpersoon bij DEFION of bel ons algemene nummer.

DEFION