Riasztás az NGINX kritikus sérülékenységeiről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ-NKI) riasztást ad ki a NGINX webszervereket érintő kritikus sérülékenységekkel kapcsolatban, tekintettel azok súlyosságára, várható kihasználására, valamint az érintett technológia széles körű elterjedtségére.

2026 november 18-án öt, az NGINX webszervereket érintő kritikus sérülékenység került nyilvánosságra, amelyek összefoglalóan **NGINX2Root** néven ismertek. A sérülékenységek sikeres kihasználása lehetővé teheti, hogy egy távoli, hitelesítéssel nem rendelkező támadó tetszőleges kódot hajtson végre az érintett kiszolgálón, az NGINX munkafolyamatának jogosultságaival.

A sérülékenységek egy további, a Linux kernel SCTP alrendszerét érintő jogosultságkiterjesztési hibával kombinálva lehetővé tehetik a rendszergazdai (root) jogosultság megszerzését, valamint bizonyos körülmények között a konténerizált környezetből történő kitörést is.

Érintett sérülékenységek

- CVE-2026-123007: A HTTP/2 protokoll adatfolyam-vezérlését érintő sérülékenység, amely távoli kódfuttatást tehet lehetővé.
- CVE-2026-123633: A HTTP/2 kapcsolatok és a háttérkiszolgálók felé továbbított kérések kezelését érintő use-after-free sérülékenység.
- CVE-2026-121810: A HTTP/3 (QUIC) protokollt és a háttérkiszolgálók felé továbbított kérések feldolgozását érintő use-after-free sérülékenység.
- CVE-2026-123634: A DNS-feloldási és alkéréskezelési folyamatokat érintő use-after-free sérülékenység, amely meghatározott proxykonfigurációk esetén használható ki.

NEMZETI KIBERBIZTONSÁGI INTÉZET
+36-1-336-4833 csirt@nki.gov.hu

- CVE-2026-113425: Az NGINX levelezési proxyfunkcióját érintő use-after-free sérülékenység, amely bizonyos hitelesítési konfigurációk esetén használható ki.

A sérülékenységek különböző NGINX-verziókat és konfigurációkat érintenek. A CVE-2026-123007 sérülékenység az NGINX 1.9.5 és 1.31.8 közötti hivatalos verzióit érinti, amennyiben a HTTP/2 protokoll engedélyezett, és a megfelelő biztonsági javítás nem került telepítésre.

Az érintettség ellenőrzése

Az NBSZ-NKI javasolja az üzemeltetett NGINX kiszolgálók verziójának, fordítási beállításainak és konfigurációjának ellenőrzését.

1. Az NGINX verziójának ellenőrzése

Az alkalmazott NGINX-verzió az alábbi paranccsal ellenőrizhető:

```
nginx -v 2>&1
```

A CVE-2026-123007 sérülékenység az 1.9.5-1.31.8 verziókat érinti. A javított kiadások közé tartozik az 1.30.7-es stabil és az 1.31.9-es mainline verzió.

Fontos, hogy egyes Linux-disztribúciók a biztonsági javításokat a verziószám módosítása nélkül is visszaportolhatják, ezért a telepített csomag pontos verzióját és a disztribúció biztonsági közleményeit is ellenőrizni szükséges.

2. A HTTP/2 modul meglétének ellenőrzése

Az alábbi paranccsal megállapítható, hogy az NGINX támogatja-e a HTTP/2 protokollt:

```
nginx -V 2>&1 | grep -- '--with-http_v2_module'
```

Amennyiben a parancs találatot ad, a HTTP/2 modul megtalálható az NGINX fordítási beállításai között. Ez önmagában nem jelenti a sérülékenység kihasználhatóságát, ehhez a protokoll engedélyezése is szükséges.

3. A HTTP/2 és HTTP/3 konfigurációjának ellenőrzése

A konfigurációban az alábbi paranccsal kereshetők az érintett protokollok engedélyezésére utaló beállítások:

```
sudo nginx -T 2>&1 | grep -E 'http2|http3|quic'
```

Különösen az alábbi konfigurációs beállítások ellenőrzése javasolt:

- `listen 443 ssl http2;`
- `http2 on;`
- `listen 443 quic;`
- `http3 on;`

4. A további érintett funkciók ellenőrzése

A többi sérülékenység kihasználhatósága meghatározott konfigurációs feltételekhez kötött. Az alábbi paranccsal ellenőrizhető az érintett funkciók használata:

```
sudo nginx -T 2>&1 | grep -E
'resolver|proxy_pass|fastcgi_pass|grpc_pass|mirror|mirror_request_body|aut
h_http|proxy on'
```

A találatok alapján szükséges megvizsgálni, hogy az adott sérülékenység kihasználásához szükséges konfigurációs feltételek együttesen teljesülnek-e.

5. A HTTP/2 külső elérhetőségének ellenőrzése

Az alábbi paranccsal ellenőrizhető, hogy az adott kiszolgáló TLS-kapcsolaton keresztül támogatja-e a HTTP/2 protokollt:

```
openssl s_client -connect PELDA.DOMAIN.HU:443 -servername PELDA.DOMAIN.HU -
alpn h2 </dev/null 2>&1 | grep 'ALPN protocol'
```

Amennyiben a kimenetben az ALPN protocol: h2 érték szerepel, a vizsgált végpont elfogadja a HTTP/2 kapcsolatokat.

A vizsgálatot lehetőség szerint a külső hálózatból, valamint közvetlenül az NGINX kiszolgáló irányában is javasolt elvégezni, mivel a köztes proxy- vagy CDN-szolgáltatások befolyásolhatják az eredményt.

Fontos: A fenti ellenőrzések az érintettség előzetes felmérését szolgálják. Egy konfigurációs direktíva jelenléte önmagában nem bizonyítja a sérülékenységet, míg a találatok hiánya nem feltétlenül zárja ki a kitettséget. Az érintettség

megállapításához a futó konfigurációt, a telepített biztonsági javításokat és a sérülékenységenként eltérő feltételeket együttesen szükséges vizsgálni.

Javasolt védelmi intézkedések

Az NBSZ-NKI az alábbi intézkedések mielőbbi végrehajtását javasolja:

- Biztonsági frissítések telepítése: Az érintett NGINX kiszolgálók frissítése az 1.30.7-es stabil, az 1.31.9-es mainline vagy újabb, javított verzióra, illetve a Linux-disztribúció által biztosított megfelelő biztonsági javítások alkalmazása.
- Érintettség felmérése: Az üzemeltetett NGINX kiszolgálók és konténerképek verzióinak, konfigurációinak és internet felőli elérhetőségének ellenőrzése.
- HTTP/2 ideiglenes letiltása: Amennyiben a biztonsági frissítés nem telepíthető azonnal, a HTTP/2 protokoll ideiglenes letiltása az érintett szolgáltatásokon. Ez a CVE-2026-123007 és CVE-2026-123633 sérülékenységek kihasználási lehetőségét szünteti meg az adott végpontokon, de a többi sérülékenység ellen nem nyújt védelmet.
- További érintett funkciók korlátozása: A HTTP/3 (QUIC), a dinamikus DNS-feloldást alkalmazó proxykonfigurációk és a levelezési proxyfunkciók felülvizsgálata, szükség esetén ideiglenes korlátozása.
- Naplóállományok és rendszertevékenységek vizsgálata: A szokatlan hálózati kapcsolatok, váratlan NGINX munkafolyamat-leállások, valamint a webszerver-folyamatok által indított gyanús parancsvégrehajtások ellenőrzése.
- Fokozott monitorozás: Az internet felől elérhető NGINX kiszolgálók kiemelt megfigyelése és az esetleges kompromittálódásra utaló események kivizsgálása.

Az NBSZ-NKI felhívja az üzemeltetők figyelmét, hogy a sérülékenységek sikeres kihasználása az érintett rendszerek kompromittálódásához vezethet, ezért kiemelten fontos a biztonsági frissítések mielőbbi telepítése, az érintettség ellenőrzése, valamint a szükséges védelmi intézkedések végrehajtása.

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

Hivatkozások:

https://xint.io/blog/nginx2root-remote-code-execution
https://thehackernews.com/2026/11/10-year-old-nginx-http2-flaw-lets.html
https://nki.gov.hu/figyelmeztetesek/serulekenysegek/cve-2026-123007
https://nki.gov.hu/figyelmeztetesek/serulekenysegek/CVE-2026-123633
https://nki.gov.hu/figyelmeztetesek/serulekenysegek/CVE-2026-121810
https://nki.gov.hu/figyelmeztetesek/serulekenysegek/CVE-2026-123634
https://nki.gov.hu/figyelmeztetesek/serulekenysegek/CVE-2026-113425

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu