TLP:CLEAR
Szabadon terjeszthető!

Riasztás az NGINX Rift sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki az NGINX webszervereket érintő, távoli kódfuttatást lehetővé tevő sebezhetőségről**.

A **CVE-2026-42945** azonosítón nyomon követett, **NGINX Rift** kódnevű sérülékenység az NGINX **széles körben használt HTTP rewrite modulját**, az ngx_http_rewrite_module-t **érinti**. A hiba akkor jelentkezhet, amikor a `rewrite` direktívát egy másik `rewrite`, `if` vagy `set` direktíva követi, és a konfiguráció név nélküli Perl Compatible Regular Expressions (PCRE) capture-csoportokat használ, például `$1` vagy `$2` formában, olyan helyettesítő karakterlánccal, amely kérdőjelet (`?`) tartalmaz.

A sérülékenység hitelesítés nélkül, **speciálisan kialakított HTTP-kéréssel** használható ki, és az NGINX worker folyamatában halom puffer túlcsordulást (heap buffer overflow) okozhat. Amennyiben az Address Space Layout Randomization (ASLR) nincs engedélyezve**, a hiba távoli kódfuttatást is lehetővé tehet** az NGINX worker folyamatában.

A sebezhetőség **az alábbi verziókat érinti, megfelelő védelem biztosítása érdekében a felhasználóknak javasolt a megjelölt verzióra való frissítés**:

- NGINX Plus R32 - R36 (a javítások az R32 P6 és az R36 P4 verziókban jelentek meg)
- NGINX Open Source 1.0.0 - 1.30.0 (javítva az 1.30.1 és 1.31.0 verziókban)
- NGINX Open Source 0.6.27 - 0.9.7 (nem terveznek javítást)
- NGINX Instance Manager 2.16.0 - 2.21.1
- F5 WAF for NGINX 5.9.0 - 5.12.1
- NGINX App Protect WAF 4.9.0 - 4.16.0
- NGINX App Protect WAF 5.1.0 - 5.8.0
- F5 DoS for NGINX 4.8.0
- NGINX App Protect DoS 4.3.0 - 4.7.0
- NGINX Gateway Fabric 1.3.0 - 1.6.2
- NGINX Gateway Fabric 2.0.0 - 2.5.1
- NGINX Ingress Controller 3.5.0 - 3.7.2
- NGINX Ingress Controller 4.0.0 - 4.0.1
- NGINX Ingress Controller 5.0.0 - 5.4.1

Amennyiben a frissítés telepítése nem megoldható, javasolt a `rewrite` **konfiguráció módosítása** az érintett `rewrite` direktívákban **a név nélküli capture-csoportok névvel ellátott capture-csoportokra** cserélésével.

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

További információk

https://thehackernews.com/2026/05/18-year-old-nginx-rewrite-module-flaw.html

https://depthfirst.com/nginx-rift

https://my.f5.com/manage/s/article/K000161019

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833