Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0164

Kwetsbaarheid verholpen in NGINX ngx_http_rewrite_module

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 18-05-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

NGINX heeft een kwetsbaarheid verholpen in het ngx_http_rewrite_module, onderdeel van zowel NGINX Plus als de Open Source editie.

Duiding

De kwetsbaarheid betreft een heap buffer overflow in het ngx_http_rewrite_module, dat verantwoordelijk is voor URL rewriting functionaliteit. Een aanvaller kan deze kwetsbaarheid misbruiken door speciaal vervaardigde HTTP-verzoeken te sturen die bepaalde rewrite directives manipuleren, wat leidt tot geheugenbeschadiging wat kan leiden tot een Denial-of-Service.

Wanneer Address Space Layout Randomization (ASLR) is uitgeschakeld, kan een niet-geauthenticeerde aanvaller mogelijk willekeurige code uitvoeren. Address Space Layout Randomization (ASLR) is een standaardfunctie van de kernel en moet doelbewust worden uitgeschakeld en dat is niet gebruikelijk. Wel is het mogelijk dat bij bepaalde lichtgewicht distributies ASLR is uitgeschakeld bij installatie ivm performance-issues. Dit soort lichtgewicht distro's is vooral populair op low end platforms als Raspberry PI.

NGINX meldt bekend te zijn met (pogingen tot) misbruik van deze kwetsbaarheid.

Oplossingen

NGINX heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://nginx.org/en/security_advisories.html
- https://access.redhat.com/security/cve/CVE-2026-42945
- https://my.f5.com/manage/s/article/K000161019
- https://nvd.nist.gov/vuln/detail/CVE-2026-42945
- https://security.alpinelinux.org/vuln/CVE-2026-42945
- https://ubuntu.com/security/notices/USN-8271-1

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-42945	9.2 CRITICAL

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-131	Incorrect Calculation of Buffer Size

Getroffen producten

NGINX
NGINX
NGINX Plus

Disclaimer