



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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.