Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0506

PRIORITEIT: HOOG

Kwetsbaarheden verholpen in NGINX door F5 Networks

Publicatiedatum: 18-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

F5 Networks heeft meerdere kwetsbaarheden verholpen in NGINX Plus en NGINX Open Source.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen en configuraties van NGINX. De belangrijkste kwetsbaarheid met kenmerk CVE-2026-123007 stelt kwaadwillenden in staat om willekeurige code uit te voeren op het onderliggende systeem.

Het NCSC verwacht dat er op korte termijn proof of concept code beschikbaar komt, waarna exploitatie op grote schaal verwacht wordt.

Oplossingen

F5 Networks heeft updates uitgebracht voor NGINX Plus en NGINX Open Source om deze kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://my.f5.com/manage/s/article/K000163925
- https://my.f5.com/manage/s/article/K000163926
- https://my.f5.com/manage/s/article/K000163927
- https://my.f5.com/manage/s/article/K000163928
- https://my.f5.com/manage/s/article/K000163930
- https://my.f5.com/manage/s/article/K000163931
- https://my.f5.com/manage/s/article/K000163932
- https://my.f5.com/manage/s/article/K000163933
- https://my.f5.com/manage/s/article/K000163934
- https://my.f5.com/manage/s/article/K000163935

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-113425	9.2 CRITICAL
CVE-2026-118899	8.7 HIGH
CVE-2026-120967	6.3 MEDIUM
CVE-2026-120993	6.9 MEDIUM
CVE-2026-121810	9.2 CRITICAL
CVE-2026-123007	9.2 CRITICAL
CVE-2026-123633	9.2 CRITICAL
CVE-2026-123634	9.2 CRITICAL
CVE-2026-123640	6.9 MEDIUM
CVE-2026-125283	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition
CWE-1289	Improper Validation of Unsafe Equivalence in Input

Getroffen producten

F5
NGINX (all other products)
NGINX Open Source

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.