



# NCSC-2026-0171

## Kwetsbaarheid verholpen in Starlette

NCSC Advisory

**PRIORITEIT: HOOG**

Gepubliceerd op: 29-05-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Er is een kwetsbaarheid verholpen in Starlette, een Python-library voor het ontwikkelen van webservices. Starlette wordt door verschillende producten gebruikt, waaronder FastAPI.

## Duiding

Een ongeauthenticeerde kwaadwillende kan de kwetsbaarheid misbruiken voor het omzeilen van authenticatie. Hierdoor kan de kwaadwillende afgeschermd URL-paden benaderen. Zodoende krijgt de kwaadwillende ongeauthenticeerde toegang tot functionaliteiten of data van een webservice die een kwetsbare Starlette-versie gebruikt.

De kwetsbaarheid wordt veroorzaakt doordat het pad in de Host-header onvoldoende wordt geverifieerd. De mogelijke impact van misbruik is afhankelijk van het soort data dat door een kwetsbare webservice wordt verwerkt en de functionaliteiten die deze service biedt.

## Oplossingen

De kwetsbaarheid is verholpen in Starlette versie 1.0.1. Applicaties die Startelle gebruiken, dienen Starlette bij te werken naar deze of een latere versie.

Indien jouw organisatie applicaties gebruikt waar Starlette onderdeel van is, zoals FastAPI, dan ben je voor beveiligingsupdates mogelijk afhankelijk van je leverancier.

Wanneer een van je applicaties een kwetsbare versie van Starlette gebruikt en het niet mogelijk is om Starlette te updaten, kan de kans op misbruik worden beperkt door de kwetsbare applicatie niet naar het internet te ontsluiten of authenticatie via een reverse proxy in te regelen.

Lees de bijgevoegde referenties voor meer informatie.

## Referenties

- <https://badhost.org/>
- <https://github.com/Kludex/starlette/security/advisories/GHSA-86qp-5c8j-p5mr>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2026-48710</a>	<b>6.5 MEDIUM</b>

## CWE's

CWE	Beschrijving
<a href="#">CWE-444</a>	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

## Getroffen producten

Kludex
starlette

## 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.