Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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 afgeschermde 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
CVE-2026-48710	**6.5 MEDIUM**

CWE's

CWE	Beschrijving
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Getroffen producten

Kludex
starlette

Disclaimer