Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0402

## Kwetsbaarheid verholpen in MongoDB

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-12-2025

**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

De ontwikkelaars van MongoDB hebben een kwetsbaarheid verholpen in MongoDB.

## Duiding

De kwetsbaarheid met kenmerk CVE-2025-14847 stelt een ongeauthenticeerde aanvaller op afstand in staat om ongeïnitialiseerd heapgeheugen uit te lezen. De oorzaak ligt in het onjuist verwerken van lengteparameters in Zlib-gecomprimeerde protocolheaders. Misbruik van de kwetsbaarheid kan leiden tot het lekken van gevoelige informatie uit het heapgeheugen, wat door een aanvaller kan worden ingezet om verdere aanvallen op het systeem uit te voeren

Onderzoekers hebben een exploit gepubliceerd waarmee CVE-2025-14847 kan worden misbruikt. Het NCSC verwacht op korte termijn actief misbruik van de kwetsbaarheid.

## Oplossingen

De ontwikkelaars van MongoDB hebben updates uitgebracht om de kwetsbaarheid te verhelpen in versie 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32 en 4.4.30.

Indien het niet mogelijk is om direct te updaten, adviseren de ontwikkelaars om als mitigerende maatregel zlib-compressie uit te schakelen en gebruik te maken van een alternatief compressie-algoritme, zoals snappy of zstd. Zie de bijgevoegde referenties voor aanvullende informatie.

## Referenties

- https://jira.mongodb.org/browse/SERVER-115508
- https://nvd.nist.gov/vuln/detail/CVE-2025-14847

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2025-14847 | 8.7 HIGH |

## CWE's

| CWE | Beschrijving |
| --- | --- |
| | |

| | |
|---|---|
| CWE-130 | Improper Handling of Length Parameter Inconsistency |

## Getroffen producten

| MongoDB |
|---|
| MongoDB |

## Disclaimer