



# NCSC-2026-0304

## ZeroDay Kwetsbaarheid verholpen in GeoTools door OpenGeo

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-08-2026

**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

GeoTools, een veelgebruikte open source Java-bibliotheek voor geospatiale data, heeft updates uitgebracht om ZeroDay SQL-injectie kwetsbaarheid te verhelpen in de uitvoering van OGC Filterfuncties bij gebruik met JDBCDataStore en andere datastores.

## Duiding

De genoemde kwetsbaarheid is een oudere kwetsbaarheid, waarvan recentelijk is gebleken dat deze niet adequaat is verholpen. De kwetsbaarheid stelde een kwaadwillende in staat om willekeurige SQL-code uit te voeren in de onderliggende database.

De ZeroDay kwetsbaarheid bevindt zich in meerdere OGC Filterfuncties die SQL-injectie mogelijk maken bij gebruik met verschillende datastore-implementaties zoals PostGIS. Hierdoor kan een aanvaller via deze functies kwaadaardige SQL-code injecteren. De kwetsbaarheden zijn aanwezig in meerdere versies van GeoTools. Als gedeeltelijke mitigatie kunnen encode-functies worden uitgeschakeld en prepared statements worden ingeschakeld om de blootstelling te verminderen.

Indien de onderliggende database draait onder verhoogde rechten, is het mogelijk om via deze kwetsbaarheid willekeurige code uit te voeren op de server, waardoor naast ongeautoriseerde database-manipulatie, ook een system take-over mogelijk kan zijn.

Onderzoekers hebben meldingen ontvangen dat kwaadwillenden de nieuwe ZeroDay onder de aandacht hebben en nemen een verhoging waar in scan- en misbruikverkeer. Op dit moment is van grootschalige ongeautoriseerde toegang of daadwerkelijk misbruik nog geen sprake.

Voor deze nieuwe ZeroDay kwetsbaarheid is (nog) geen CVE-id bekend gesteld.

## Oplossingen

De leverancier heeft updates uitgebracht in versies 35.1, 34.5 en 33.6 om deze beveiligingsproblemen aan te pakken. Zie bijgevoegde referenties voor meer informatie.

## Referenties

➤ <https://github.com/geotools/geotools/security/advisories/GHSA-mqjf-5f49-2fjh>

## Kwetsbaarheden

| CVE                                 | CVSS Score   |
|-------------------------------------|--------------|
| <a href="#">&gt; CVE-2023-25158</a> | 9.8 CRITICAL |

## CWE's

| CWE                         | Beschrijving                                                                         |
|-----------------------------|--------------------------------------------------------------------------------------|
| <a href="#">&gt; CWE-89</a> | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |

## Getroffen producten

| GeoTools |
|----------|
| GeoTools |

## 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.