



NCSC-2025-0393

Kwetsbaarheid verholpen in GeoServer

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-12-2025

Revisie: 1.0.1

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

Update Revisie 1

We hebben bericht ontvangen dat de genoemde versies in de GeoServer advisory onder 'Resolution' nog kwetsbaar zijn. Updaten naar de nieuwste versie 2.28.1 verhelpt voor zover bekend wel deze kwetsbaarheid.

Feiten

OSGeo heeft een kwetsbaarheid verholpen in GeoServer.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop GeoServer XML-input verwerkt, specifiek via de `/geoserver/wms` GetMap-operatie. Onjuiste sanitatie van XML-input stelt aanvallers in staat om gevoelige bestanden openbaar te maken of Denial-of-Service-aanvallen uit te voeren met behulp van op maat gemaakte XML-input. Er zijn gevallen van actief misbruik van deze kwetsbaarheid bekend.

Oplossingen

OSGeo heeft updates uitgebracht om de kwetsbaarheid te verhelpen. In tegenstelling tot wat in de referentie staat adviseert het NCSC om te updaten naar versie 2.28.1, aangezien de genoemde versies in de advisory de kwetsbaarheid nog steeds bevatten.

Referenties

➤ <https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-58360	6.9 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-611	Improper Restriction of XML External Entity Reference

Getroffen producten

GeoServer

GeoServer

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.