



NCSC-2026-0343

Kwetsbaarheden verholpen in GeoNetwork door OpenGeo

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 07-09-2026

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

OpenGeo heeft meerdere kwetsbaarheden verholpen in GeoNetwork, een open-source catalogusapplicatie, specifiek in versies 4.4.5 tot en met 4.4.11 en versies voorafgaand aan 4.4.12 en 4.2.17.

Duiding

De eerste kwetsbaarheid betreft een reflected cross-site scripting (XSS) in de publieke, niet-geauthenticeerde cataloguszoekfunctie. Dit wordt veroorzaakt door onvoldoende sanering van de uiconfig queryparameter, waardoor een aanvaller JavaScript kan injecteren en uitvoeren in de browsercontext van gebruikers. De tweede kwetsbaarheid betreft een onveilige configuratie van de XSLT-processor die het mogelijk maakt voor gebruikers met uploadrechten om willekeurige besturingssysteemcommando's uit te voeren via geüploade .xsl-bestanden. De derde kwetsbaarheid betreft een onbeveiligde API-endpoint die het mogelijk maakt voor niet-geauthenticeerde aanvallers om willekeurige .xsl- of .zip-bestanden te uploaden, wat ongeautoriseerde schrijfrechten op de server kan veroorzaken en mogelijk leidt tot servercompromittering.

Oplossingen

OpenGeo heeft updates uitgebracht in GeoNetwork versies 4.4.12 en 4.2.17 die deze kwetsbaarheden verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://docs.geonetwork-opensource.org/4.2/overview/change-log/version-4.2.17>
- <https://docs.geonetwork-opensource.org/4.4/overview/change-log/version-4.4.12>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-57582	8.2 HIGH
➤ CVE-2026-58400	9.1 CRITICAL
➤ CVE-2026-63219	8.6 HIGH

CWE's

CWE	Beschrijving
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
➤ CWE-94	Improper Control of Generation of Code ('Code Injection')
➤ CWE-470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
➤ CWE-862	Missing Authorization

Getroffen producten

Open Source
GeoNetwork
geonetwork
core-geonetwork

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.