Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0526

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in GeoServer

Publicatiedatum: 27-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

GeoServer heeft 17 kwetsbaarheden verholpen, waarvan GeoServer er één als kritiek en twaalf als hoog heeft beoordeeld.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-129245 heeft een CVSS-score van 9.2 en betreft een voorspelbare cryptografische sleutel binnen de 'remember-me'-functionaliteit. Een kwaadwillende die beschikt over de benodigde gegevens kan de kwetsbaarheid misbruiken om een geldige beheerderssessie te vervalsen en daarmee administratieve toegang te verkrijgen.

GeoServer beschrijft daarnaast een aanvalsketen waarbij vijf kwetsbaarheden worden gecombineerd. Naast CVE-2026-129245 betreft het CVE-2026-129244 (CVSS 6.9), CVE-2026-129243 (CVSS 8.8), CVE-2026-120705 (CVSS 8.6) en CVE-2026-129242 (CVSS 8.6). Door misbruik van deze kwetsbaarheden kan een niet-geauthenticeerde kwaadwillende op afstand uiteindelijk willekeurige code uitvoeren op een kwetsbare GeoServer-installatie.

De overige kwetsbaarheden betreffen onder meer Server-Side Request Forgery (SSRF), ongeautoriseerde bestandstoegang, het schrijven van bestanden, authenticatie- en autorisatieomzeiling en Cross-Site Scripting (XSS). De kwetsbaarheid met kenmerk CVE-2026-120706 heeft een CVSS-score van 8.2 en kan onder specifieke omstandigheden leiden tot SSRF en het uitlezen van bestanden. CVE-2026-120704 heeft een CVSS-score van 7.2 en kan door een kwaadwillende met beheerdersrechten worden misbruikt om willekeurige code uit te voeren.

De kwetsbaarheden met kenmerk CVE-2026-129294 en CVE-2026-129293 kunnen eveneens worden gecombineerd tot een aanvalsketen die leidt tot opgeslagen Cross-Site Scripting (XSS). Voor een deel van de kwetsbaarheden moeten specifieke extensies of modules zijn geïnstalleerd.

Oplossingen

GeoServer heeft beveiligingsupdates uitgebracht om de kwetsbaarheden te verhelpen. De kwetsbaarheden zijn verholpen in GeoServer 3.0.2, 2.28.6 en 2.27.7. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://geoserver.org/vulnerability/2026/11/23/cve-update.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-120701	
CVE-2026-120702	
CVE-2026-120703	
CVE-2026-120704	
CVE-2026-120705	
CVE-2026-120706	
CVE-2026-120707	
CVE-2026-120708	
CVE-2026-120709	
CVE-2026-129240	
CVE-2026-129242	
CVE-2026-129243	
CVE-2026-129244	
CVE-2026-129245	
CVE-2026-129293	
CVE-2026-129294	
CVE-2026-120710	

CWE's

CWE	Beschrijving
CWE-91	XML Injection
CWE-94	Improper Control of Generation of Code
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-321	Use of Hard-coded Cryptographic Key
CWE-502	Deserialization of Untrusted Data
CWE-863	Incorrect Authorization

Getroffen producten

Geoserver
Geoserver

Open Source
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.