Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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
CVE-2023-25158	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

GeoTools
GeoTools

Disclaimer