Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0274

Kwetsbaarheid verholpen in GeoServer

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 05-07-2024
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

Er is een Proof-of-Concept-code (PoC) gepubliceerd waarmee de kwetsbaarheid kan worden aangetoond.

Feiten

De ontwikkelaars van GeoServer hebben een kwetsbaarheid verholpen.

Voor deze kwetsbaarheid is Proof-of-Concept-code (PoC) op internet verschenen.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop XPath expressies door de API worden verwerkt en stelt een kwaadwillende in staat om met speciaal geprepareerde XPath expressies een command-injection uit te voeren en zo code uit te voeren met rechten van de applicatie.

Proof-of-Concept-Code is beschikbaar om de kwetsbaarheid aan te tonen. Systemen waarbij de API publiek toegankelijki is lopen hiermee verhoogd risico. De API in kwestie is normaal gesproken niet standaard bereikbaar vanaf publieke netwerken.

Oplossingen

De ontwikkelaars van GeoServer hebben updates uitgebracht om de kwetsbaarheid te verhelpen in GeoServer 2.24.4, 2.25.2 en 2.23.6.

Ook zijn mitigerende maatregelen gepubliceerd om de kwetsbaarheid te beperken indien uitrol van de updates (nog) niet mogelijk is. Indien het bestand gt-complex-x.y.jar (x.y. zijnde de versienummering, afhankelijk van de versie van de GeoServer-software) van de server wordt verwijderd is misbruik niet mogelijk. Dit kan echter gevolgen hebben voor de werking van de installatie. Maak hiervoor een separate risico-inschatting per systeem.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://github.com/advisories/GHSA-6jj6-gm7p-fcvv

Kwetsbaarheden

CVE	CVSS Score

CVE-2024-36401	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Getroffen producten

geoserver
geoserver

Disclaimer