

GitHub Advisory Database / GitHub Reviewed / CVE-2023-25157

GeoServer OGC Filter SQL Injection Vulnerabilities

Critical severity

GitHub Reviewed

Published on Feb 21, 2023 in geoserver/geoserver • Updated on Feb 22, 2023

Vulnerability details

Dependabot alerts 0

Package	Affected versions	Patched versions
 org.geoserver.community:gs-jdbcconfig (Maven)	< 2.21.4 >= 2.22.0, < 2.22.2	2.21.4 2.22.2

Description

Impact

GeoServer includes support for the OGC Filter expression language and the OGC Common Query Language (CQL) as part of the Web Feature Service (WFS) and Web Map Service (WMS) protocols. CQL is also supported through the Web Coverage Service (WCS) protocol for ImageMosaic coverages.

SQL Injection Vulnerabilities have been found with:

- `PropertyIsLike` filter, when used with a String field and any database DataStore, or with a PostGIS DataStore with encode functions enabled
- `strEndsWith` function, when used with a PostGIS DataStore with encode functions enabled
- `strStartsWith` function, when used with a PostGIS DataStore with encode functions enabled
- `FeatureId` filter, when used with any database table having a String primary key column and when prepared statements are disabled
- `jsonArrayContains` function, when used with a String or JSON field and with a PostGIS or Oracle DataStore (GeoServer 2.22.0+ only)
- `DWithin` filter, when used with an Oracle DataStore

Patches

- GeoSever 2.21.4
- GeoServer 2.22.2
- GeoServer 2.20.7
- GeoServer 2.19.7
- GeoServer 2.18.7

Workarounds

- Disabling the PostGIS Datastore *encode functions* setting to mitigate `strEndsWith` , `strStartsWith` vulnerabilities (Like filters have no mitigation, if there is a string field in the feature type published).
- Enabling the PostGIS DataStore *preparedStatements* setting to mitigate the `FeatureId` vulnerability.

References

- [OGC Filter SQL Injection Vulnerabilities](#) (GeoTools)
- [OGC Filter Injection Vulnerability Statement](#) (GeoServer Blog)

References

- [GHSA-7g5f-wrx8-5ccf](#)
- <https://nvd.nist.gov/vuln/detail/CVE-2023-25157>
- [geoserver/geoserver@ 145a8af](#)

Severity

Critical

9.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS score

54.684% (98th percentile)

Weaknesses

CWE-89

CVE ID

CVE-2023-25157

GHSA ID

GHSA-7g5f-wrx8-5ccf

Source code

[geoserver/geoserver](#)

Credits

 sikeoka

Analyst

This advisory has been edited. [See History](#).

See something to contribute? [Suggest improvements for this vulnerability](#).

 Published by the [National Vulnerability Database](#) on Feb 21, 2023

 Published to the GitHub Advisory Database on Feb 22, 2023

 Reviewed on Feb 22, 2023

 Last updated on Feb 22, 2023



© 2024 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)