Security Advisory 2024-068

Critical Vulnerabilities in GeoServer and GeoTools

July 11, 2024 — v1.0

TLP:CLEAR

History:

- 11/07/2024 — v1.0 – Initial publication

Summary

On July 2, 2024, several critical vulnerabilities were addressed in GeoServer and GeoTools. These vulnerabilities can result in arbitrary code execution through the unsafe evaluation of user-supplied XPath expressions [1,2,3]. It is recommended updating as soon as possible.

Technical Details

The vulnerability CVE-2024-36401, with a CVSS score of 9.8, allows Remote Code Execution (RCE) flaw by unauthenticated users via specially crafted input to a default GeoServer installation. This issue arises from the unsafe evaluation of property names as XPath expressions due to a flaw in the GeoTools library API, which GeoServer relies upon [1].

The vulnerability CVE-2024-36404, with a CVSS score of 9.8, is a Remote Code Execution (RCE) flaw against the GeoTools library. This vulnerability occurs when certain methods use the commons-jxpath library to evaluate XPath expressions supplied within user inputs. The commons-jxpath library has the capability to execute arbitrary code embedded within these XPath expressions [2].

Affected Products

CVE-2024-36401 affects the following packages

- org.geoserver.web:gs-web-app
- org.geoserver:gs-wfs
- org.geoserver:gs-wms

and their versions:

- From version 2.24.0 up to, but not including, version 2.24.4
- From version 2.25.0 up to, but not including, version 2.25.2
- All versions prior to 2.23.6
**CVE-2024-36404** affects the following packages

- org.geotools.xsd:gt-xsd-core
- org.geotools:gt-app-schema
- org.geotools:gt-complex

and their versions:

- From version 30.0 up to, but not including, version 30.4
- From version 31.0 up to, but not including, version 31.2
- All versions prior to 29.6

**Recommendations**

CERT-EU strongly recommends updating to the latest versions by following the instructions given by the vendor [1,2].

**Workaround and Mitigation**

GeoServer has issued a workaround and mitigation measures depending on the release version.

The workaround is to remove the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version. This will remove the vulnerable code from GeoServer but may impact other functionalities. A list of mitigation measures is available [1,2].

**References**

