National Cyber Security Centre

2407090141-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in GeoServer (CVE-2024-36401, CVSSv3: 9.8)

Tuesday 9th July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-07-01T16:15:00
Vendor: GeoServer
Product: GeoServer
CVE ID: CVE-2024-36401
CVSS3.0 Score[1]**:** 9.8
EPSS[2]**:** 0.961890000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-36401

Summary: GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions. The vulnerability, tracked as CVE-2024-36401 can lead to execution of arbitrary code.

Products Affected

- 2.25.x, versions prior to 2.25.2
- 2.24.x, versions prior to 2.24.4
- versions prior to 2.23.6

Impact

This vulnerability can lead to Remote Code Execution.

Recommendations

Versions 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the ‘gt-complex-x.y.jar‘ file from the GeoServer where ‘x.y‘ is the GeoTools version (e.g., ‘gt-complex-31.1.jar‘ if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed.

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates.

Additional information on recommendations and mitigation’s for CVE-2024-36401 can be found in the respective link(s):
https://github.com/advisories/GHSA-6jj6-gm7p-fcvv

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre