NVD DB Update

CVE-2024-36401 - Score: 9.8

Components:

geotools geotools *
geoserver geoserver *

Description:

GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.22.6, 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 GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.22.6, 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.

Main problems:

95 no CWE Description available