Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical GeoTools RCE Flaw Exploited in Geoserver Attacks

Date of Publication	Admiralty Code	TA Number
July 18, 2024	A1	TA2024276

Summary

First Seen: June 2024
Affected Products: GeoServer, GeoTools
Impact: A critical Remote Code Execution (RCE) vulnerability in GeoTools, identified as CVE-2024-36404, has been disclosed. This 9.8 severity RCE vulnerability is caused by the unsafe evaluation of property names as XPath expressions. Another related flaw affecting GeoServer is CVE-2024-36401. This vulnerability stems from the GeoTools library API, which GeoServer relies on to evaluate property and attribute names for feature types.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-36401	OSGeo GeoServer GeoTools Eval Injection Vulnerability	GeoServer	✗	✓	✓
CVE-2024-36404	OSGeo GeoTools Remote Code Execution Vulnerability	GeoTools	✗	✗	✓

Vulnerability Details

#1 A critical remote code execution (RCE) vulnerability in the GeoTools library, identified as CVE-2024-36404, has been discovered. Concurrently, CVE-2024-36401, which affects the GeoServer integration of GeoTools, is actively being exploited in attacks. GeoTools is an open-source Java library that provides tools and APIs for geospatial data processing and analysis, and it is extensively used in various applications and frameworks, including GeoServer.

#2 CVE-2024-36404 arises from improper input validation, allowing a remote attacker to send a specially crafted request to execute arbitrary code on the target system. This RCE risk occurs if an application uses specific GeoTools functions to evaluate XPath expressions supplied by user input. The issue lies in methods that pass XPath expressions to the commons-jxpath library, which can execute arbitrary code if the XPath expressions come from user input.

#3 GeoTools' API, used by GeoServer, evaluates property and attribute names for feature types by passing them to the commons-jxpath library. This library's ability to execute arbitrary code when evaluating XPath expressions poses a significant security risk. Originally intended for complex feature types, this XPath evaluation is incorrectly applied to simple feature types as well, impacting all GeoServer instances.

#4 The Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2024-36401 to its Known Exploited Vulnerabilities (KEV) Catalog, warning that the flaw is being actively exploited in attacks. CISA has instructed federal agencies to patch their servers by August 5, 2024. The active exploitation of CVE-2024-36401 was first observed on July 9. Around 16,000 GeoServer servers are exposed online, with the majority located in the United States, China, Romania, Germany, and France.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-36401	GeoServer: Versions prior to 2.23.6, 2.24.0 to 2.24.3, and 2.25.0 to 2.25.1.	cpe:2.3:a:geoserver:geoserver:*:*:*:*:*:*:*:*	CWE-95
CVE-2024-36404	GeoTools: Versions prior to 29.6, 30.0 to 30.3, and 31.0 to 31.1.	cpe:2.3:a:geotools:geotools:*:*:*:*:*:*:*:*	CWE-95

Recommendations

Update: Users are strongly advised to upgrade to the latest versions of GeoServer and GeoTools, which contain patches addressing this vulnerability. The patched versions include GeoServer 2.23.6, 2.24.4, and 2.25.2, and GeoTools 29.6, 30.4, and 31.2.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the RCE vulnerability, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1129 Shared Modules	T1190 Exploit Public-Facing Application

Patch Details

Users are strongly advised to upgrade to the latest versions of GeoServer and GeoTools. The patched versions include GeoServer 2.23.6, 2.24.4, and 2.25.2, and GeoTools 29.6, 30.4, and 31.2.

Patch Links:
https://sourceforge.net/projects/geotools/files/
https://geoserver.org/download/

Workaround: As a workaround, the 'gt-complex' JAR file can be removed from GeoTools. This action will eliminate the vulnerable code but may disrupt some functionality if the gt-complex module is required by an extension in use. On GeoServer, the gt-complex JAR file is named 'gt-complex-x.y.jar', where x.y represents the GeoTools version.

References

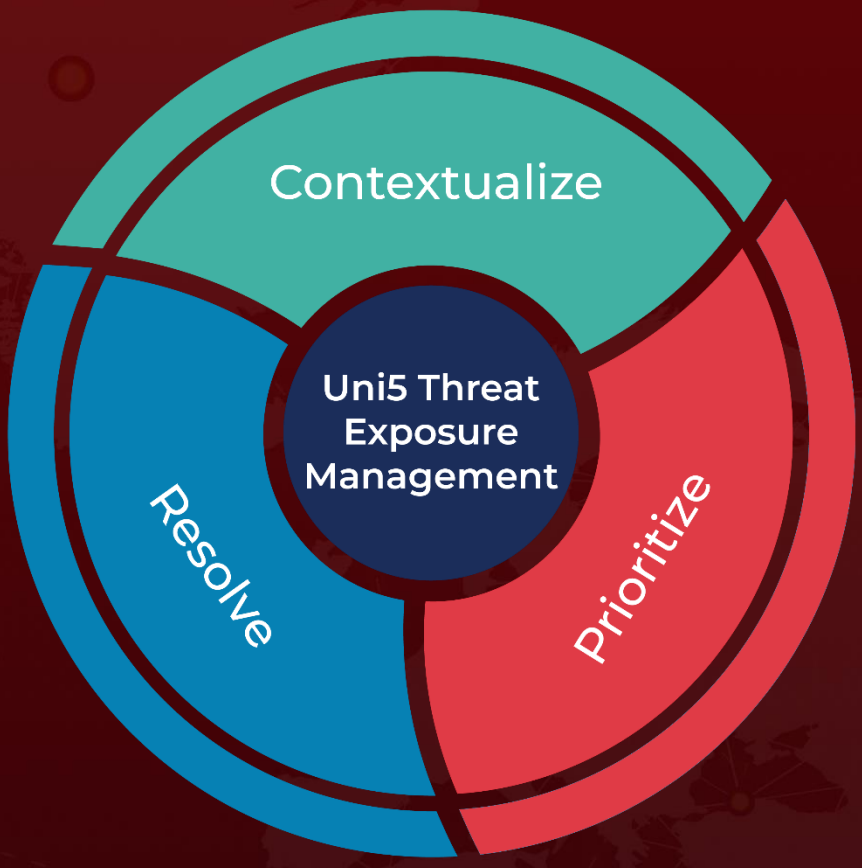
https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv

https://github.com/geotools/geotools/security/advisories/GHSA-w3pj-wh35-fq8w

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 18, 2024 • 8:00 AM

More at www.hivepro.com