مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE Vulnerability in GeoServer

Tracking #:432316019

Date:05-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GeoServer issued security updates to address a remote Code Execution (RCE) vulnerability in GeoServer.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-36401** | CVSS Score: 9.8 | Critical
- 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.

Affected versions:

- >= 2.24.0, < 2.24.4
- >= 2.25.0, < 2.25.2
- < 2.23.6

Patched versions:

- 2.24.4
- 2.25.2
- 2.23.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest security updates at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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