مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in Apache Wicket

Tracking #:432316788

Date:27-01-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Wicket, a widely-used Java-based web application framework, which could be exploited to launch denial-of-service (DoS) attacks on affected web applications.

## TECHNICAL DETAILS:

**Vulnerabilities Details:**

- **CVE-2024-53299**
- A critical vulnerability exists in Apache Wicket. This flaw allows attackers to trigger a memory leak, potentially leading to denial-of-service (DoS) attacks on affected web applications.
- The vulnerability affects the request handling core of Apache Wicket, enabling attackers to overwhelm the server by repeatedly sending requests to server resources. This can cause memory exhaustion, resulting in application crashes or unresponsiveness.

**Affected Versions**

- Wicket 7.0.0 through 7.18.*
- Wicket 8.0.0-M1 through 8.16.*
- Wicket 9.0.0-M1 through 9.18.*
- Wicket 10.0.0-M1 through 10.2.*

**Fixed Versions:**

- Wicket 9.19.0
- Wicket 10.3.0

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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://nvd.nist.gov/vuln/detail/CVE-2024-53299