مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Apache Causeway

Tracking #:432318045

Date:21-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability in Apache Causeway, a widely used framework for rapidly building domain-driven Java applications. This vulnerability allows authenticated attackers to exploit unsafe Java deserialization mechanisms and execute arbitrary code within affected applications.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-64408**
- **Severity:** Critical
- **Component Affected:** ViewModel functionality
- The vulnerability stems from unsafe Java deserialization mechanisms accessible via user-controlled URL parameters in applications utilizing Apache Causeway's ViewModel feature. This functionality generates dynamic web interfaces and REST APIs based on domain logic, and in affected versions, reconstructs serialized object graphs from incoming requests.
- **Impact:** Authenticated remote attackers may achieve arbitrary code execution through crafted URL parameters containing malicious serialized payloads.

Affected Versions

Apache Causeway:

- 2.0.0 through 3.4.0
- 4.0.0-M1

Fixed Version

- Apache Causeway 3.5.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache Causeway.

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-2025-64408