مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Spring Security

Tracking #:432317287

Date:20-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Spring Security that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-41232**
- A security vulnerability exists in Spring Security when using AspectJ-based method security. The flaw arises from how Spring Security handles annotations on private methods. When developers place method-level security annotations on private methods while using AspectJ, the framework may fail to enforce the intended security restrictions, potentially allowing unauthorized access.
- Successful exploitation of this vulnerability could allow an unauthorized user to invoke methods that are intended to be protected by Spring Security's method-level security mechanisms. This could lead to:
    - Data leakage
    - Unauthorized modification of data
    - Elevation of privilege
    - Other security breaches, depending on the specific application and the functionality of the affected methods.

Affected Versions:

- Spring Security: 6.4.0 - 6.4.5

Fixed Versions:

- Spring Security version 6.4.6 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Spring Security.

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://spring.io/security/cve-2025-41232