مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Spring Security

Tracking #:432317006

Date:24-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Spring Security, a widely used framework for Java-based applications. These vulnerabilities could lead to authorization bypass and weak password enforcement, posing serious security risks.

TECHNICAL DETAILS:

Vulnerability Details:

1. CVE-2025-22223: Authorization Bypass in Method Security Annotations

- **Description:** Spring Security may not correctly locate method security annotations on parameterized types or methods. This can result in an authorization bypass, allowing unauthorized users to invoke restricted methods.
- **Impact:** Attackers may gain unauthorized access to sensitive application functionalities.
- **Affected Versions:** Spring Security 6.4.0 – 6.4.3
- **Fixed Versions:** Spring Security 6.4.4.

2. CVE-2025-22228: Weak Password Enforcement in BCryptPasswordEncoder

- **Description:** BCryptPasswordEncoder.matches(CharSequence, String) incorrectly returns true for passwords larger than 72 characters if the first 72 characters match the expected password.
- **Impact:** Enables password truncation attacks, potentially bypassing authentication.
- **Affected Versions:** Spring Security 5.7.0 – 6.4.3
- **Fixed Versions:** Spring Security 6.3.8, 6.4.4 (for OSS users) or apply enterprise support patches for older versions.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2025-22223
- https://spring.io/security/cve-2025-22228