مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Spring Security

Tracking #:432316172

Date:22-08-2024

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-2024-38810- Missing Authorization When Using @AuthorizeReturnObject**
- **Severity: High**
- A security vulnerability exists in Spring Security that could allow unauthorized access to sensitive data within affected applications. This vulnerability arises from a flaw in the way Spring Security handles method security annotations when objects are wrapped using @AuthorizeReturnObject or the AuthorizationAdvisorProxyFactory.

Conditions for Vulnerability

The vulnerability only affects applications that meet all of the following conditions:

1. Using AnnotationAwareAspectJAutoProxyCreator for auto-proxy creation
2. Having at least one FactoryBean in the application context
3. Enabling method security with @EnableMethodSecurity
4. Wrapping objects using @AuthorizeReturnObject or AuthorizationAdvisorProxyFactory
5. Using @PreFilter, @PostFilter, @PreAuthorize, or @PostAuthorize on those wrapped objects

Affected Versions:

- Spring Security 6.3.0 and 6.3.1

Fixed Versions:

- Spring Security version 6.3.2 or later

RECOMMENDATIONS:

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

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-2024-38810