مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Authorization Bypass Vulnerability in Spring WebFlux Applications

Tracking #:432316447

Date:29-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in Spring WebFlux applications utilizing Spring Security, enabling potential authorization bypass for static resources.

TECHNICAL DETAILS:

A critical vulnerability has been identified in Spring WebFlux applications utilizing Spring Security, enabling potential authorization bypass for static resources.

Vulnerability Details:

- **CVE ID: CVE-2024-38821**
- **CVSS Score**: 9.1,Critical
- The vulnerability arises in Spring WebFlux applications that employ Spring Security authorization rules on static resources. Under certain circumstances, these rules can be bypassed, leading to unauthorized access. For this vulnerability to be exploitable, the following conditions must be met:
  - The application must be a WebFlux application.
  - Spring's static resources support must be in use.
  - A non-permitAll authorization rule must be applied to the static resources.

Affected Versions:

- 5.7.0 - 5.7.12
- 5.8.0 - 5.8.14
- 6.0.0 - 6.0.12
- 6.1.0 - 6.1.10
- 6.2.0 - 6.2.6
- 6.3.0 - 6.3.3
- Older, unsupported versions are also affected

Fixed Versions:

- 5.7.13
- 5.8.15
- 6.0.13
- 6.1.11
- 6.2.7
- 6.3.4

RECOMMENDATIONS:

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

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-2024-38821