مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Path Traversal Vulnerability in Spring Framework

Tracking #:432316423
Date:22-10-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a path traversal vulnerability has been identified in the Spring Framework, affecting applications utilizing the WebMvc.fn and WebFlux.fn functional web frameworks.

## TECHNICAL DETAILS:

A path traversal vulnerability, identified as **CVE-2024-38819**, has been discovered in the Spring Framework, affecting applications that utilize the **WebMvc.fn** and **WebFlux.fn** functional web frameworks.

**Vulnerability Details:**

- **CVE Identifier**: CVE-2024-38819
- **CVSS Score**: 7.5 (High)
- Attackers can exploit this vulnerability remotely without authentication by crafting malicious HTTP requests that leverage directory traversal sequences to access any file on the server's file system that is readable by the Spring application process.
- The potential impact includes unauthorized access to sensitive information such as:
  - Configuration files
  - Application logs
  - User credentials
- **Affected Versions**:
  - Spring Framework 5.3.0 to 5.3.40
  - Spring Framework 6.0.0 to 6.0.24
  - Spring Framework 6.1.0 to 6.1.13
- **Fixed Versions**:
  - For users on 5.3.x, upgrade to 5.3.41.
  - For users on 6.0.x, upgrade to 6.0.25.
  - For users on 6.1.x, upgrade to 6.1.14.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends users of affected Spring Framework versions should upgrade to the respective patched 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-2024-38819