مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Spring Framework Path Traversal Vulnerability

Tracking #:432316286

Date:16-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Spring Framework that could be exploited to gain unauthorized access to sensitive files on a server, potentially leading to data breaches and system compromise.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2024-38816
- **CVSS Score:** 7.5 High
- A path traversal vulnerability exists in Spring Framework's handling of static resources served through WebMvc.fn or WebFlux.fn. By crafting malicious HTTP requests, attackers can bypass security measures and retrieve arbitrary files from the server's file system.
- Successful exploitation of this vulnerability could allow attackers to access sensitive files, steal sensitive information, and gain unauthorized access to the server, potentially leading to the execution of malicious code.

Affected Versions:

- Spring Framework 5.3.0 to 5.3.39
- Spring Framework 6.0.0 to 6.0.23
- Spring Framework 6.1.0 to 6.1.12
- Older and unsupported versions

Fixed Versions:

- Spring Framework 5.3.40
- Spring Framework 6.0.24
- Spring Framework 6.1.13

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-38816