مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Vulnerability in Spring Framework

Tracking #:432317385

Date:17-06-2025

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 vulnerability in Spring Framework that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-41234**
- Severity: Medium (CVSS 6.5)
- A vulnerability has been identified in the Spring Framework that could allow an attacker to perform a reflected file download (RFD) attack. This occurs when a “Content-Disposition” header is set with a non-ASCII charset, and the filename attribute is derived from unsanitized user-supplied input.
- Successful exploitation could allow an attacker to trick a user into downloading a file containing malicious content, potentially leading to arbitrary code execution or other malicious activities on the victim’s system.

Affected versions	Fix versions	Availability
6.2.x	6.2.8	OSS
6.1.x	6.1.21	OSS
6.0.x	6.0.29	Commercial

RECOMMENDATIONS:

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

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-2025-41234