مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Spring Cloud Data Flow

Tracking #:432316190
Date:28-08-2024

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Spring Cloud Data Flow, a widely used tool for cloud-based data processing. This vulnerability could be exploited to execute malicious code on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22263**
- CVSS Base Score: 8.8 HIGH
- Arbitrary file write vulnerability exists in Spring Cloud Data Flow, a microservices-based data processing platform. This vulnerability allows an attacker with access to the Skipper server API to write arbitrary files to the server's filesystem, potentially leading to system compromise.
- A proof-of-concept (PoC) exploit available for CVE-2024-22263, highlighting the severity of the vulnerability.
- Successful exploitation of this vulnerability could allow an attacker to:
    - Write arbitrary files to the server's filesystem, including sensitive files or system binaries.
    - Execute arbitrary code on the server, potentially leading to complete system compromise.

Affected Versions:

- Spring Cloud Skipper 2.11.0 - 2.11.2
- Spring Cloud Skipper 2.10.x

Fixed Versions:

- **Spring Cloud Skipper 2.11.x:** Upgrade to 2.11.3
- **Spring Cloud Skipper 2.10.x:** Upgrade to 2.11.3

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://nvd.nist.gov/vuln/detail/CVE-2024-22263