مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Apache Struts

Tracking #:432316630

Date:13-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in Apache Struts and this vulnerability allows attackers to upload malicious files, potentially leading to remote code execution, unauthorized access, or system compromise.

TECHNICAL DETAILS:

A critical file upload logic flaw has been identified in Apache Struts versions 2.0.0 to versions before 6.4.0 (CVE-2024-53677). This vulnerability allows attackers to upload malicious files, potentially leading to remote code execution, unauthorized access, or system compromise.

Vulnerability Details:

- **CVE-2024-53677**
- CVSS score of 9.5 Critical
- An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution.

Affected Versions:

- Struts 2.0.0 - Struts 2.3.37 (EOL), Struts 2.5.0 - Struts 2.5.33, Struts 6.0.0 - Struts 6.3.0.2

Fixed Versions:

- Struts 6.4.0 or greater and use Action File Upload Interceptor.

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://cwiki.apache.org/confluence/display/WW/S2-067