مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

DoS Vulnerability in Apache Struts

Tracking #:432318091

Date:04-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Denial-of-Service (DoS) vulnerability in Apache Struts 2 caused by a file leak during multipart/form-data processing.

TECHNICAL DETAILS:

A newly disclosed vulnerability, CVE-2025-64775, affects multiple maintained and end-of-life versions of Apache Struts 2, a widely used Java web application framework. The flaw stems from improper handling of multipart/form-data requests, resulting in a file leak during upload processing. Under certain conditions, this leak can cause unbounded file accumulation on disk, leading to resource exhaustion and ultimately a Denial of Service (DoS) condition.

Exploitation requires only the ability to send crafted HTTP multipart requests. This makes the vulnerability particularly impactful for public-facing Struts applications handling file uploads or forms using multipart data.

Vulnerability Details

- CVE Identifier-CVE-2025-64775
- Base Score: 7.5 HIGH
- Affected Software
  - Struts 2.0.0 through Struts 2.3.37 (EOL)
  - Struts 2.5.0 through Struts 2.5.33 (EOL)
  - Struts 6.0.0 through Struts 6.7.0
  - Struts 7.0.0 through Struts 7.0.3
- Recommendation
  - Upgrade to Struts 6.8.0 at least or 7.1.1

RECOMMENDATIONS:

- All users are strongly advised to upgrade immediately to prevent DoS attacks.

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/S2-068