December 15, 2023

Cyber Alert

This is a technical bulletin intended for technical audiences.

Summary

On December 4, 2023, Apache released a security bulletin to address a critical vulnerability (CVE-2023-50164) affecting Apache Struts 2 versions 2.0.0 to 2.3.37, 2.5.0 to 2.5.32 and 6.0.0 to 6.3.0.

Technical Details

On December 4, 2023, Apache released a security bulletin to address a critical vulnerability (CVE-2023-50164) affecting Apache Struts 2 versions 2.0.0 to 2.3.37, 2.5.0 to 2.5.32 and 6.0.0 to 6.3.0. The vulnerability is rated as a 9.8 on the Common Vulnerability Scoring System (CVSS3) and can allow a malicious actor to upload malicious files and perform remote code execution.

The Canadian Centre for Cyber Security (Cyber Centre) and our cyber security partners have published alerts and advisories encouraging all organizations to apply patches to the affected products. Historically, vulnerabilities impacting Struts 2 have been significant due to the broad adoption of the Apache Struts 2 framework within the industry.

The Cyber Centre has verified publicly available proof of concepts (POCs) and is aware of malicious activity within Canada.

The Cyber Centre strongly recommends that organizations patch the affected Apache Struts 2 systems to versions 2.5.33 and 6.3.0.2 or greater at their earliest opportunity. Apache Struts versions 2.0.0 to 2.3.37 are vulnerable but are no longer supported. Impacted organizations are encouraged to update any unsupported products to a supported version.

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

The Cyber Centre recommends organizations:

- Verify the existence of Apache Struts on their hosts, monitor for signs of exploitation and patch software using Struts 2 as soon as possible.
    - For Linux systems, the lsof command may be used to identify commonly named struts files loaded within applications with the following command:

        - sudo lsof -w | grep -i "struts2.*\.jar"

    - For Windows systems, it may be possible to determine the location of commonly named Apache Struts archives by using the following Powershell command replacing <DRIVEPATH> for each mounted drive.

        - Get-ChildItem -Path <DRIVEPATH> -Recurse -ErrorAction SilentlyContinue -Filter '*struts*.jar'

    - This technique of detection is not a definitive method in the identification of all impacted systems and products. The Cyber Centre strongly recommends that organizations monitor vendor advisory spaces to receive notifications of impact along with mitigation recommendations and patches.

In addition, the Cyber Centre strongly recommends that organizations review and implement the Cyber Centre's Top 10 IT Security Actions with an emphasis on the following topics:

- Consolidate, monitor, and defend Internet gateways
- Patch operating systems and applications
- Isolate web-facing applications

Please notify VRM with any questions or concerns you may have.

Partner Reporting

- ACSC - Critical Vulnerability in popular Java framework Apache Struts2 – Alert
- CISA - The Apache Software Foundation Updates Struts 2 – Alert
- NCSC-NZ - Cyber Security Alert: CVE affecting Apache Struts 2 – Advisory

References

- CVE-2023-50164
- Apache Struts 2 Security Bulletin - S2-066
- CCCS AV23-748 – Apache security advisory
- The Apache Software Foundation Updates Struts 2
- Critical vulnerability in popular Java framework Apache Struts2
- Cyber Security Alert: CVE affecting Apache Struts 2
- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)
- VRM Vulnerability Reports