December 8, 2023

Overall rating: Critical

BRITISH
COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of an Apache Struts vulnerability. The vulnerability affects Apache Struts versions prior to 6.3.0.2 & 2.5.33.

Technical Details

Apache Struts version update addresses a potential security vulnerability identified as CVE-2023-50164 and described in S2-066. 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. Users are recommended to upgrade to versions Struts 2.5.33 or Struts 6.3.0.2 or greater to fix this issue.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

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

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2023-50164
- Apache Struts versions 6.3.0.2 & 2.5.33
- S2-066

- VRM Vulnerability Reports