S2-066

Created by Lukasz Lenart, last modified on Dec 09, 2023

Summary

File upload logic is flawed, and allows an attacker to enable paths with traversals

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Remote Code Execution
Maximum security rating	critical
Recommendation	Upgrade to Struts 2.5.33 or Struts 6.3.0.2 or greater
Affected Software	Struts 2.0.0 - Struts 2.3.37 (EOL), Struts 2.5.0 - Struts 2.5.32, Struts 6.0.0 - Struts 6.3.0
Reporters	Steven Seeley of Source Incite
CVE Identifier	CVE-2023-50164

Problem

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.

Solution

Upgrade to Struts 2.5.33, 6.3.0.2 or greater.

Backward compatibility

No issues expected when upgrading to Struts 2.5.33 or 6.3.0.2

Workaround

n/a

No labels