National Cyber Security Centre

2312120117-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Apache Struts: File Upload Component Directory Traversal Vulnerability (CVE-2023-50164)

Wednesday 13th December, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Published: 2023-12-07, 09:15:00
Vendor: Apache Software Foundation
Product: Apache Struts
CVSSv3[1]**:** 9.8

Summary: 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.

More information related to this issue can be found at the following link(s):

- https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lfwtqhj
- https://www.openwall.com/lists/oss-security/2023/12/07/1

Products Affected

- Apache Struts 2.0.0 through 2.5.32
- Apache Struts 6.0.0 through 6.3.0.1

Impact

Common Weakness Enumeration (CWE)[2]**:** CWE-552 Files or Directories Accessible to External Parties

Present in CISA Known Exploited Vulnerability (KEV)[3] **catalog:** NO

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and upgrade to versions Struts 2.5.33 or Struts 6.3.0.2 or greater.

Additional recommendations and mitigation's for the CVE can be found in the respective links below:

- https://lists.apache.org/thread/yh09b3fkf6vz5d6jdgrlvmg60lfwtqhj
- https://www.openwall.com/lists/oss-security/2023/12/07/1

[1] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie