



An Lárionad Náisiúnta
Cibearshlándaála
National Cyber
Security Centre

NCSC #2412120142

NCSC Advisory

A Critical vulnerability exist in
Apache Software Foundation, Struts
(CVSS: 9.5)

12th, December 2024

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.



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

TLP: CLEAR

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



Description

CVE ID: CVE-2024-53677

Published: 2024-12-11

Vendor: Apache Software Foundation

Product: Apache Struts

CVSS3.0 Score¹: 9.5

Products affected

Product	Version
Apache Struts	2.0.0 < 6.4.0

Impact

File upload logic is flawed in Apache Struts. This issue affects Apache Struts from 2.0.0 before 6.4.0. Users are recommended to upgrade to version 6.4.0, which fixes the issue.

Common Weakness Enumeration (CWE)²:

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

¹ <https://www.first.org/cvss/v3.0/specification-document>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



TLP: CLEAR

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Apache Software Foundation

- <https://nvd.nist.gov/vuln/detail/CVE-2024-53677>
- <https://www.cve.org/CVERecord?id=CVE-2024-53677>
- <https://cwiki.apache.org/confluence/display/WW/S2-067>

