NCSC Advisory

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

12th, December 2024

STATUS: TLP:CLEAR

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

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

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 Score[1]: 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) catalog[3]: 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

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

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

Recommedations

The NCSC strongly reccommends 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

Tom Johnson House, Beggar's Bush, Dublin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333   **E** info@ncsc.gov.ie

ncsc.gov.ie

TLP: CLEAR

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre