CYBER ADVISORY

TLP:CLEAR

20 December 2024

Apache Struts 2 Remote Code Execution Vulnerability

CVE-2024-54677 | Apache Struts | Code Execution | Critical Vulnerabilities

The California Cyber Security Integration Center (Cal-CSIC) has become aware of a critical Apache Struts 2 vulnerability, tracked as CVE-2024-53677 [1] (CVSS 3.1 score: 9), that is being actively exploited globally.[2] This vulnerability allows threat actors to upload arbitrary payloads to susceptible instances, which could then be leveraged to run commands, exfiltrate data, or download additional payloads for follow-on exploitation.[3] This vulnerability is similar to CVE-2023-50164, a 2023 Struts 2 upload vulnerability that threat actors began exploiting soon after public proof-of-concept (POC) release.[4]

Cal-CSIC recommends users upgrade to version 6.4.0 and migrate to new file upload mechanism to remediate this vulnerability.

For further information on patching this vulnerability, please refer to:

S2-067 - Apache Struts 2 Wiki - Apache Software Foundation

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This advisory is based on information obtained from trusted sources, such as NIST, the Australian government and reputable cybersecurity news websites.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] National Institute of Standards and Technology, "CVE-2024-53677 Detail" https://nvd.nist.gov/vuln/detail/CVE-2024-53677: accessed 18 December 2024
[2] Australian Signals Directorate, "Critical Vulnerability in Popular Java Framework Apache Struts 2" https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerability-in-popular-java-framework-apache-struts2: accessed 18 December 2024
[3] The Hacker News, "Patch Alert: Critical Apache Struts Flaw Found, Exploitation Attempts Detected", https://thehackernews.com/2024/12/patch-alert-critical-apache-struts-flaw.html: accessed 18 December 2024
[4] The Hacker News, "New Critical RCE Vulnerability Discovered in Apache Struts 2 – Patch Now" https://thehackernews.com/2023/12/new-critical-rce-vulnerability.html: accessed 18 December 2024