aDvens

Security for the greater good

Newscast

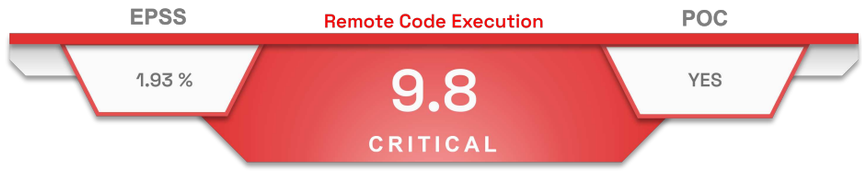
Critical vulnerability in Apache Struts

2023-12-14 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-50164



On 4 December 2023, Apache released a security advisory concerning a vulnerability discovered in *Apache Struts 2*, identified as CVE-2023-50164.

A data control flaw in the *Strusts ActionSupport* class, allows a remote unauthenticated attacker to upload a malicious file to a targeted folder and execute it.

The CERT-FR have warned, in their advisory of 13 December 2023, of the existence of an proof-of-concept available in the wild and of possible exploitation attemps..

Attempts to exploit this flaw have been observed by the ANSSI.

Type of vulnerability

- **CWE-552**: Files or Directories Accessible to External Parties

Risk

- Remote Code Execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

Versions Struts :

- Struts versions 2.x prior to 2.5.33
- Struts versions 6.x prior to 6.3.0.2

Recommendations

- Update Apache Struts to version 2.5.33, 6.3.0.2 or later.
- Further information is available in the editor's security advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- https://cwiki.apache.org/confluence/display/WW/s2-066
- https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-013/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50164