CERT-EU

Security Advisory 2023-095

Critical Vulnerability in Apache Struts

December 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/12/2023 — v1.0 – Initial publication*

Summary

On December 7, 2023, The Apache Struts group released an update addressing a critical security vulnerability in Apache Struts. This vulnerability could lead, under some circumstances, to remote code execution [1,2].

It is recommended to upgrade to a not vulnerable version as soon as possible.

Technical Details

The vulnerability, identified as **CVE-2023-50164** with a CVSS score of 9.8 [3], may allow an attacker to manipulate file upload parameters to enable path traversal. Under some circumstances this may allow the attacker to upload a malicious file that can be used to perform remote code execution.

Affected Products

This vulnerability affects Apache Struts versions 2.0.0 through 2.5.32 and 6.0.0 through 6.3.0.1 [2].

Recommendations

It is recommended to upgrade to a not vulnerable version as soon as possible.

References

[1] https://www.helpnetsecurity.com/2023/12/08/cve-2023-50164/

[2] https://cwiki.apache.org/confluence/display/WW/S2-066

[3] https://www.tenable.com/cve/CVE-2023-50164