S2-069

Created by Lukasz Lenart, last modified on Dec 19, 2025

Summary

XXE vulnerability in XWork component

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Disclosure of Data, Denial of Service, Server Side Request Forgery
Maximum security rating	Important
Recommendation	Upgrade to Struts 6.1.1 at least
Affected Software	▪ Struts 2.0.0 through Struts 2.3.37 (EOL) ▪ Struts 2.5.0 through Struts 2.5.33 (EOL) ▪ Struts 6.0.0 through Struts 6.1.0
Reporters	ZAST.AI - https://zast.ai
CVE Identifier	CVE-2025-68493

Problem

Parsing of XML configuration in XWork component does not validate XML in proper way and it's vulnerable to XML external entity (XXE) injection.

Solution

Upgrade to Struts 6.1.1 at least.

Backward compatibility

This change is backward compatible.

Workaround

Users unable to upgrade immediately can mitigate XXE either by:

- using a custom **SAXParserFactory**: set `xwork.saxParserFactory=` to a custom factory class that disables external entities by default

or

- defining **JVM-level configuration**: configure the JVM's default XML parser to disable external entities via system properties (set to empty string to block all protocols):

```
-Djavax.xml.accessExternalDTD=""
-Djavax.xml.accessExternalSchema=""
```

```
-Djavax.xml.accessExternalStylesheet=""
```

No labels