S2-028

Summary

Use of a JRE with broken URLDecoder implementation may lead to XSS vulnerability in Struts 2 based web applications.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Affects of a cross-site scripting vulnerability.
Maximum security rating	Important
Recommendation	Upgrade runtime JRE to a recent major version, preferably 1.8. Alternatively upgrade to Struts 2.3.28
Affected Software	Struts 2.0.0 - Struts Struts 2.3.24.1
Reporter	WhiteHat Security (whitehatsec.com)
CVE Identifier	CVE-2016-4003

Problem

When using a single byte page encoding such as ISO-8895-1, an attacker might submit a non-spec URL-encoded parameter value including multi-byte characters.

Struts 2 used the standard JRE URLDecoder to decode parameter values. Especially JRE 1.5's URLDecoder implementation seems to be broken to the point that this non-spec encoding isn't rejected / filtered. In later JREs the issue was fixed, best known solution is found in JRE 1.8.

Solution

Upgrade runtime JRE/JDK, preferably to the most recent 1.8 version.

Alternatively upgrade to Struts 2.3.28, which includes and uses a safe URLDecoder implementation from Apache Tomcat

Backward compatibility

No issues expected when upgrading to Struts 2.3.28

Workaround

Use UTF-8 for page and parameter encoding.

Further Reference

~~WW-4507~~ - Struts 2 XSS vulnerability with <s:textfield> CLOSED