

S2-007

Summary

User input is evaluated as an OGNL expression when there's a conversion error

Who should read this	All Struts 2 developers
Impact of vulnerability	Remote Code Execution
Maximum security rating	Important
Recommendation	Developers should either upgrade to Struts 2.2.3.1 or apply the configuration changes described below
Affected Software	Struts 2.0.0 - Struts 2.2.3
Original JIRA Tickets	WW-3668
Reporter	Hideyuki Suzumi
CVE Identifier	-

Problem

User input is evaluated as an OGNL expression when there's a conversion error. This allows a malicious user to execute arbitrary code. A more detailed description is found in the referenced [JIRA ticket](#).

Solution

Upgrade to [Struts 2.2.3.1](#).