Security Export

Mon Dec 31, 2018

Exported by: admin

Package type: Maven

Component name: com.opensymphony:xwork:2.0.6

Summary	Severity	Type	Provider	Component	Infected Version	Fix Version	Edited
The TextParseUtil.translateVariables method in Apache Struts 2.x before 2.3.20 allows remote attackers to execute arbitrary code via a crafted OGNL expression with ANTLR tooling.	Medium	security	JFrog	com.opensymphony:xwork	2.0.4 <= Version <= 2.1.3		2018-12-12T14:55:00+02:00
The OGNL extensive expression evaluation capability in XWork in Struts 2.0.0 through 2.1.8.1, as used in Atlassian Fisheye, Crucible, and possibly other products, uses a permissive whitelist, which allows remote attackers to modify server-side context objects and bypass the "#" protection mechanism in ParameterInterceptors via the (1) #context, (2) #_memberAccess, (3) #root, (4) #this, (5) #_typeResolver, (6) #_classResolver, (7) #_traceEvaluations, (8) #_lastEvaluation, (9) #_keepLastEvaluation, and possibly other OGNL context variables, a different vulnerability than CVE-2008-6504.	Medium	security	JFrog	com.opensymphony:xwork	2.0.4 <= Version <= 2.1.3		2018-12-12T14:54:49+02:00
Multiple cross-site scripting (XSS) vulnerabilities in XWork in Apache Struts 2.x before 2.2.3, and OpenSymphony XWork in OpenSymphony WebWork, allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) an action name, (2) the action attribute of an s:submit element, or (3) the method attribute of an s:submit element.	Low	security	JFrog	com.opensymphony:xwork	2.0.4 <= Version <= 2.1.3		2018-12-12T14:54:50+02:00