S2-011

Summary

Long request parameter names might significantly promote the effectiveness of DOS attacks

Who should read this	All Struts 2 developers
Impact of vulnerability	Denial-of-Service attacks
Maximum security rating	Important
Recommendation	Developers should upgrade to Struts 2.3.4.1
Affected Software	Struts 2.0.0 - Struts 2.3.4
Original JIRA Tickets	WW-3860
Reporter	Johno Crawford
CVE Identifier	CVE-2012-4387

Problem

Request parameters handled by Struts 2 are effectively treated as OGNL expressions. A possible DOS attacker might craft requests to a Struts 2 based application with extremely long parameter names. OGNL evaluation of the parameter name then will consume significant CPU cycles, thus promoting the effectiveness of the DOS attack.

Solution

As of Struts 2.3.4.1, parameter name length is limited to a maximum of 100 characters. This configuration may be customized by providing the newly introduced parameter "paramNameMaxLength" to the ParametersInteceptor configuration.

Thanks to Johno Crawford for the provided patch.

Please upgrade to Struts 2.3.4.1.