Security Bulletins

The following security bulletins are available:

- S2-001 — Remote code exploit on form validation error
- S2-002 — Cross site scripting (XSS) vulnerability on <s:url> and <s:a> tags
- S2-003 — XWork ParameterInterceptors bypass allows OGNL statement execution
- S2-004 — Directory traversal vulnerability while serving static content
- S2-005 — XWork ParameterInterceptors bypass allows remote command execution
- S2-006 — Multiple Cross-Site Scripting (XSS) in XWork generated error pages
- S2-007 — User input is evaluated as an OGNL expression when there's a conversion error
- S2-008 — Multiple critical vulnerabilities in Struts2
- S2-009 — ParameterInterceptor vulnerability allows remote command execution
- S2-010 — When using Struts 2 token mechanism for CSRF protection, token check may be bypassed by misusing known session attributes
- S2-011 — Long request parameter names might significantly promote the effectiveness of DOS attacks
- S2-012 — Showcase app vulnerability allows remote command execution
- S2-013 — A vulnerability, present in the includeParams attribute of the URL and Anchor Tag, allows remote command execution
- S2-014 — A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks
- S2-015 — A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution.
- S2-016 — A vulnerability introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:" allows remote command execution
- S2-017 — A vulnerability introduced by manipulating parameters prefixed with "redirect:"/"redirectAction:" allows for open redirects
- S2-018 — Broken Access Control Vulnerability in Apache Struts2
- S2-019 — Dynamic Method Invocation disabled by default
- S2-020 — Upgrade Commons FileUpload to version 1.3.1 (avoids DoS attacks) and adds 'class' to exclude params in ParametersInterceptor (avoid ClassLoader manipulation)
- S2-021 — Improves excluded params in ParametersInterceptor and CookieInterceptor to avoid ClassLoader manipulation
- S2-022 — Extends excluded params in CookieInterceptor to avoid manipulation of Struts' internals
- S2-023 — Generated value of token can be predictable
- S2-024 — Wrong excludeParams overrides those defined in DefaultExcludedPatternsChecker
- S2-025 — Cross-Site Scripting Vulnerability in Debug Mode and in exposed JSP files
- S2-026 — Special top object can be used to access Struts' internals
- S2-027 — TextParseUtil.translateVariables does not filter malicious OGNL expressions
- S2-028 — Use of a JRE with broken URLDecoder implementation may lead to XSS vulnerability in Struts 2 based web applications.
- S2-029 — Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.
- S2-030 — Possible XSS vulnerability in I18NInterceptor
- S2-031 — XSLTResult can be used to parse arbitrary stylesheet
- S2-032 — Remote Code Execution can be performed via method: prefix when Dynamic Method Invocation is enabled.
- S2-033 — Remote Code Execution can be performed when using REST Plugin with ! operator when Dynamic Method Invocation is enabled.
- S2-034 — OGNL cache poisoning can lead to DoS vulnerability
- S2-035 — Action name clean up is error prone
- S2-036 — Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution (similar to S2-029)
- S2-037 — Remote Code Execution can be performed when using REST Plugin.
- S2-038 — It is possible to bypass token validation and perform a CSRF attack
- S2-039 — Getter as action method leads to security bypass
- S2-040 — Input validation bypass using existing default action method.
- S2-041 — Possible DoS attack when using URLValidator
- S2-042 — Possible path traversal in the Convention plugin
- S2-043 — Using the Config Browser plugin in production
- S2-044 — Possible DoS attack when using URLValidator
- S2-045 — Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.
- S2-046 — Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)
- S2-047 — Possible DoS attack when using URLValidator (similar to S2-044)
- S2-048 — Possible RCE in the Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x series
- S2-049 — A DoS attack is available for Spring secured actions

- S2-050 — A regular expression Denial of Service when using URLValidator (similar to S2-044 & S2-047)
- S2-051 — A remote attacker may create a DoS attack by sending crafted xml request when using the Struts REST plugin
- S2-052 — Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads
- S2-053 — A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals
- S2-054 — A crafted JSON request can be used to perform a DoS attack when using the Struts REST plugin
- S2-055 — A RCE vulnerability in the Jackson JSON library