Security Bulletins

Security impact levels

The Apache Struts Security Team rates the impact of each security flaw that affects Struts. We've chosen a rating scale quite similar to those used by other Apache projects in order to be consistent. Basically the goal of the rating system is to answer the question *How worried should I be about this vulnerability?*

Critical

A vulnerability rated with a **Critical** impact is one which could potentially be exploited by a remote attacker to get Struts to execute an arbitrary code. These are the sorts of vulnerabilities that could be exploited automatically by worms/hackers regardless if developers paid attention to keep their code safe and followed advices from the Security Guide.

Important

A vulnerability rated as **Important** impact is one which could result in the compromise of data or availability of the application. For Struts this includes issues that allow an easy remote code execution because developers didn't pay attention to treat users' inputs as unsecure and used it in the application logic.

Moderate

A vulnerability is likely to be rated as **Moderate** if there is significant mitigation to make the issue less of an impact. This might be because the flaw does not affect likely configurations, or it is a configuration that isn't widely used, or where a remote user must be authenticated in order to exploit the issue.

Low

All other security flaws are classed as a **Low** impact. This rating is used for issues that are believed to be extremely hard to exploit, or where an exploit gives minimal consequences.

Published 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
- S2-056 — A crafted XML request can be used to perform a DoS attack when using the Struts REST plugin
- S2-057 — Possible Remote Code Execution when alwaysSelectFullNamespace is true (either by user or a plugin like Convention Plugin) and then: results are used with no namespace and in same time, its upper package have no or wildcard namespace and similar to results, same possibility when using url tag which doesn't have value and action set and in same time, its upper package have no or wildcard namespace.
- S2-058 — Previous Security Bulletins contained incorrect affected release version ranges.
- S2-059 — Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.
- S2-060 — Access permission override causing a Denial of Service when performing a file upload
- S2-061 — Forced OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution - similar to S2-059.
- S2-062 — Forced OGNL evaluation, when evaluated on raw not validated user input in tag attributes, may lead to remote code execution - same as S2-061.
- S2-063 — DoS via OOM owing to not properly checking of list bounds.
- S2-064 — DoS via OOM owing to no sanity limit on normal form fields in multipart forms.
- S2-065 — Excessive disk usage during file upload
- S2-066 — File upload logic is flawed, and allows an attacker to enable paths with traversals