

# S2-017

## Summary

A vulnerability introduced by manipulating parameters prefixed with "redirect:"/"redirectAction:" allows for open redirects

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Open redirect
Maximum security rating	Important
Recommendation	Developers should immediately upgrade to <a href="#">Struts 2.3.15.1</a>
Affected Software	Struts 2.0.0 - Struts 2.3.15
Reporter	Takeshi Terada of Mitsui Bussan Secure Directions, Inc.
CVE Identifier	<a href="#">CVE-2013-2248</a>

## Problem

The Struts 2 DefaultActionMapper used to support a method for short-circuit navigation state changes by prefixing parameters with "redirect:" or "redirectAction:", followed by a desired redirect target expression. This mechanism was intended to help with attaching navigational information to buttons within forms.

In Struts 2 before 2.3.15.1 the information following "redirect:" or "redirectAction:" can easily be manipulated to redirect to an arbitrary location.

## Proof of concept

In the Struts Showcase App, open following URLs.

1. `http://host/struts2-showcase/fileupload/upload.action?redirect:http://www.yahoo.com/`
2. `http://host/struts2-showcase/modelDriven/modelDriven.action?redirectAction:http://www.google.com/%23`

## Solution

DefaultActionMapper was changed to drop the features involved with "redirect:"/"redirectAction:"-prefixed parameters completely - see also [S2-016](#).



### Backward Compatibility

After upgrading to Struts >= 2.3.15.1, applications using the "redirect:" / "redirectAction:" functionality will no longer work properly. Please investigate your code to replace such expressions with proper fixed navigation rules.



It is strongly recommended to upgrade to [Struts 2.3.15.1](#), which contains the corrected Struts2-Core library.