S2-050

Summary

A regular expression Denial of Service when using URLValidator (similar to S2-044 & S2-047)

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible DoS attack when using URLValidator
Maximum security rating	Low
Recommendation	Upgrade to Struts 2.5.13 or Struts 2.3.34
Affected Software	Struts 2.3.7 - Struts 2.3.33, Struts 2.5 - Struts 2.5.12
Reporter	Adam Cazzolla <acazzolla at sonatype dot com>, Jonathan Bullock <jonbullock at gmail dot com>
CVE Identifier	CVE-2017-9804

Problem

The previous fix issued with S2-047 was incomplete. If an application allows enter an URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL.

Solution

Upgrade to Apache Struts version 2.5.13 or 2.3.34.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

Instead of using the default RegEx provided by the `UrlValidator` you can use the below one:

```
"^(?:https?|ftp):\\/\\/" +
"(?:(?:[a-z0-9$_.+!*'(),;?&=\\-]|%[0-9a-f]{2})+" +
"(?::(?:[a-z0-9$_.+!*'(),;?&=\\-]|%[0-9a-f]{2})+)?" +
"@)?#?" +
"(?:(?:(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\\.)*" +
"[a-z][a-z0-9-]*[a-z0-9]" +
"|(?:(?:[1-9]?\\d|1\\d{2}|2[0-4]\\d|25[0-5])\\.){3}" +
"(?:[1-9]?\\d|1\\d{2}|2[0-4]\\d|25[0-5])" +
")(?::\\d+)?" +
")(?:(?:\\/(?:[a-z0-9$_.+!*'(),;:@&=\\-]|%[0-9a-f]{2})*)*" +
"(?:\\?(?:[a-z0-9$_.+!*'(),;:@&=\\-\\/:]|%[0-9a-f]{2})*)?)?" +
"(?:#(?:[a-z0-9$_.+!*'(),;:@&=\\-]|%[0-9a-f]{2})*)?" +
"$"
```