Redmine - Defect #19117

XSS Vulnerability in Flash rendering

2015-02-16 21:31 - Jan from Planio www.plan.io

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Fixed	**Affected version:**	

Description

Summary

There one one confirmed and several potential XSS vulnerabilities in Redmine's flash rendering.

Description

When rendering flash messages, Redmine unconditionally marks the rendered messages as html_safe. This leads to all html special characters in the flash message to be rendered as HTML unless they are manually escaped beforehand.

In several places in Redmine, the message is not sufficiently escaped and allows the rendering of raw, user-supplied values.

Example exploit:

Given a user with the following string configured as the email address (which is accepted by the mail validations):

```
">&lt;script&gt;alert('Vulnerable!')&lt;/script&gt;"a@a.bc
```

When that user sends himself a test mail using the admin/test_mail action, the configured email is pushed unescaped in the flash message, resulting in the included javascript to be executed.

This can be used in a targeted attack as a reflected XSS to perform actions as an administrator.

The attached patch also fixes other places where potentially unsafe information is passed in a flash message, including an issue similar to the one described above concerning mail registration.

This vulnerability is in Redmine since at least 2.3, possibly much longer. It is advised to backport the patch to all supported versions of Redmine and to release updated versions.

Credits

This issue was discovered by Holger Just of Planio.

Solution

Attach the patch against current Redmine trunk (redmine:r14014) attached to this mail.

Associated revisions

Revision 14016 - 2015-02-17 18:47 - Jean-Philippe Lang

Escape flash messages (#19117).

Revision 14017 - 2015-02-17 19:00 - Jean-Philippe Lang

Merged r14016 (#19117).

History

#1 - 2015-02-17 19:06 - Jean-Philippe Lang

Committed in trunk (r14016) and 2.6-stable (r14017), thanks for reporting this out.

As for any XSS vulnerability, I'll add an entry to the Security_Advisories page for this but I'll mark it as low severity as it could hardly be used for an effective attack.

#2 - 2015-02-18 01:10 - Jan from Planio www.plan.io

Thanks!

#3 - 2015-10-07 21:32 - Jean-Philippe Lang

- Status changed from New to Closed

- Resolution set to Fixed

#4 - 2015-12-07 10:00 - Jan from Planio www.plan.io

- Project changed from 2 to Redmine

- Category set to Security

Moving to public project, so it becomes visible.

Files

0001-Fix-potential-XSS-in-flash-rendering.patch	2.33 KB	2015-02-16	Jan from Planio www.plan.io