

Redmine - Patch #20203

The test email action should use POST only (CSRF protection)

2015-06-29 16:42 - Holger Just

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Jean-Philippe Lang	% Done:	0%
Category:	Security	Estimated time:	0.00 hour
Target version:	2.6.6		
Description Right now, an attacker can craft cross-site requests to a Redmine instance under the active session of an administrator which would allow it to send a large amount of test emails to this user. This is possible with a simple img tag like this: The attached patch fixes this vulnerability by changing the enforced HTTP request method from GET to POST. The patch was extracted from Planio . It applies cleanly on today's trunk.			

Associated revisions

Revision 14389 - 2015-06-29 18:09 - Jean-Philippe Lang

The test email action should only be accessible with POST (#20203).

Revision 14400 - 2015-07-05 12:29 - Jean-Philippe Lang

Merged r14389 (#20203).

Revision 14401 - 2015-07-05 12:30 - Jean-Philippe Lang

Merged r14389 (#20203).

Revision 14402 - 2015-07-05 12:30 - Jean-Philippe Lang

Merged r14389 (#20203).

History

#1 - 2015-06-29 17:58 - Jean-Philippe Lang

- Category set to Security
- Assignee set to Jean-Philippe Lang
- Target version set to 2.6.6

#2 - 2015-06-29 18:09 - Jean-Philippe Lang

- Status changed from New to Resolved

Patch committed with an additional change to the functional test, thanks.

#3 - 2015-06-29 18:10 - Jean-Philippe Lang

- Subject changed from The test email action /admin/test_email should only be accessible with POST to protect it with the CSRF protection system to The test email action should use POST only (CSRF protection)

#4 - 2015-07-05 12:30 - Jean-Philippe Lang

- Status changed from Resolved to Closed

Files

0001-Send-test-email-to-admins-with-POST.patch	2.95 KB	2015-06-29	Holger Just
--	---------	------------	-------------