OpenNebula - Bug #5502
Script injection in SPICE viewer (only Firefox)

10/26/2017 09:07 AM - Abel Coronado

Status:	Closed	**Start date:**	10/26/2017
Priority:	Normal	**Due date:**	
Assignee:	Abel Coronado	**% Done:**	100%
Category:	Sunstone	**Estimated time:**	0.00 hour
Target version:	Release 5.4.3		
Resolution:	fixed	**Pull request:**	
Affected Versions:	Development		

Description

SPICE viewer use title parameter (VM name) to insert in the DOM HTML.

When you click on a new tab, the url is like this
http://localhost:9869/spice?host=localhost&port=29876&token=q1men35mijak0k6pryde&password=null&encrypt=n&title=spice-24

If the name of your machine is:

> *</title><script>alert('hacked')</script>*

Or inject the script in the url:

> *title=</title><script>alert('hacked')</script>*

This will happen
js-injection.png

Malicious characters should be escaped to avoid this (e.g. <, >)

Associated revisions

Revision 7ca14d2d - 10/26/2017 09:09 AM - Abel Coronado

B #5502: Script injection in SPICE viewer (#546)

Revision bcefb74d - 10/26/2017 09:10 AM - Abel Coronado

B #5502: Script injection in SPICE viewer (#546)

(cherry picked from commit 7ca14d2d8984a9a50d2140b7a13693a6a3fdd4ea)

History

#1 - 10/26/2017 09:12 AM - Ruben S. Montero

- Status changed from Pending to Closed

- Resolution set to fixed

Files

js-injection.png	74.6 KB	10/26/2017	Abel Coronado