XWiki Platform / XWIKI-23472

Reflected Cross-Site Scripting (XSS) in page history compare

Details

Type:	Bug	Resolution:	Fixed
Priority:	Critical	Fix Version/s:	18.0.0-rc-1, 17.10.1, ... (2)
Affects Version/s:	10.4-rc-1		
Component/s:	Component		
Labels:	attack_xss, attacker_socialeng, security		
Environment:	stable-postgres-tomcat Docker image		
Tests:	Unit		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Similar issues:			

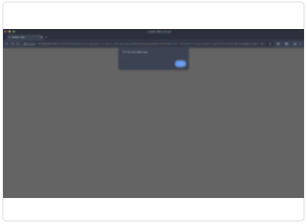
Description

The rev1 and rev2 parameters in page history compare are vulnerable to unauthenticated reflected XSS attacks.

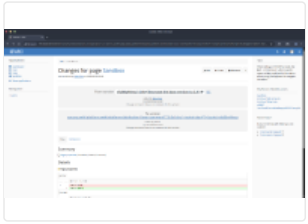
Below is an example payload for the Sandbox pages.

http://<host>/bin/view/Sandbox/?viewer=changes&rev1=9.1&rev2=xar%3aorg.xwiki.platform%3axwiki-platform-distribution-flavor-common%2f17.6.0q1che%27%3E%3Cscript%3Ealert(1)%3C%2fscript%3Evfu80q44msz&form_token=VX4OGRD4Qszx2m2Vt08FFA&languag
platform-distribution-flavor-common%2F17.6.0&rev1=9.1

Attachments



Screenshot_2025-08-20_13
20/Aug/25 05:30 40 kB



Screenshot_2025-08-20_13
20/Aug/25 05:31 193 kB

Issue Links

is caused by

XWIKI-15129 Add navigation (previous/next version) buttons in the changes view CLOSED

is related to

XWIKI-21095 RXSS through revision parameter in content menu CLOSED

links to

Security Advisory

Activity

Newest first

Michael Hamann added a comment - 01/Dec/25 15:57

There is an important part missing in the reproduction steps: the page must have at least two revisions, so if you test on a fresh instance, make sure you edit the Sandbox page at least once. I've just thought I couldn't reproduce this anymore because I was testing on a fresh instance where the Sandbox page hadn't been modified.

Michael Hamann added a comment - 01/Sep/25 11:53

I can confirm this issue and I've also just tested that the form_token isn't actually necessary to exploit this, so the crafted URLs work for any user.

People

Assignee:

Michael Hamann

Reporter:

Mike Cole

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

Dates

Created:

20/Aug/25 05:33

Updated:

6 days ago 14:17

Resolved:

02/Dec/25 16:15

Date of First Response:

01/Sep/25 11:53 AM