



XSS in the attachment history

Details

Type:	Bug	Resolution:	Fixed
Priority:	Blocker	Fix Version/s:	14.3-rc-1, (1)
Affects Version/s:	1.1 M1		
Component/s:	Web - Templates & Resources		
Labels:	attack_xss attacker_account bugfixingday regression security		
Tests:	Unit		
Development Priority:	High		
Difficulty:	Unknown		
Documentation:	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-mxf2-4r22-5hq9		
Documentation in	N/A		
Release Notes:			
Similar issues:			

Description

Steps to reproduce:

1. Create a file ".jpg" locally (any image will do).
2. Attach it to a wiki page.
3. Click on the attachments button at the bottom of the page.
4. Click on the version number next to the filename to display the history.

Expected result:

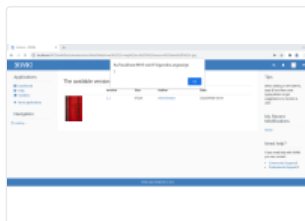
1. The history is displayed and the full filename is displayed in the title.

Actual result:

1. An alert is displayed again and the filename in the title of the history isn't fully displayed.

This demonstrates a persistent XSS vulnerability in the attachment history displayer (i.e., `viewattachrev.vm`) which should be exploitable with just write access to the user profile. As always, this can be used for privilege escalation when a user with, e.g., programming rights visits the attachment history by modifying the user profile through the injected JavaScript with the rights of the visiting user.

Attachments



history-XSS.png

06/Apr/22 11:48

92 kB

Issue Links

is caused by

[XWIKI-9000](#) Error when clicking on "View attachment history" for an attachment when not using legacy oldcore **CLOSED**

relates to

[XWIKI-19667](#) The move attachment form is missing escaping and some translations **CLOSED**

links to

▼ Activity



▼ Thomas Mortagne added a comment - 14/Apr/22 14:33 - edited

There are two bad escaping in viewattachrev.vm template:


- one introduced by <https://github.com/xwiki/xwiki-platform/commit/eb28cdaa96a84ac50282f322b2d98cb6762a8778#diff-4c6a0e234332dbf66c9c6c6ff09f528f589ff1e952d8cf39d58e335aaafff79fR4> (<https://jira.xwiki.org/browse/XWIKI-9000>) in XWiki 5.0RC1 and which affects all attachments types
- another much older introduced for which I can't go back to the origin (older than XWiki 1.1) which affects only images

▼ People

Assignee:

 Thomas Mortagne 

Reporter:

 Michael Hamann 

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

▼ Dates

Created:

06/Apr/22 11:41

Updated:

08/Sep/22 14:30

Resolved:

14/Apr/22 17:06

Date of First Response:

14/Apr/22 2:33 PM