XWiki Platform XWIKI-19559

The fact that a user is inactive is far from being taken into account everywhere

Details

Type:	Bug	Resolution:	Fixed
Priority:	Blocker	Fix Version/s:	13.10.5, (1)
Affects Version/s:	1.1 M3		
Component/s:	Old Core		
Labels:	attack_escalation attacker_account bugfixingday security		
Tests:	Integration		
Difficulty:	Unknown		
Documentation:	N/A		
Documentation in Release Notes:	N/A		
Similar issues:			

Description

Currently, a disabled user is still authenticated and set in the standard context and only really taken into account in XWiki#prepareDocuments which generate an exception for all actions but only

```
if (!((action.equals("skin") && (doc.getSpace().equals("skins") || doc.getSpace().equals("resources")))
                  || ((action.equals("skin") || action.equals("download") || action.equals("ssx") || action.equals("jsx"))
                      && getRightService().hasAccessLevel("view", XWikiRightService.GUEST_USER_FULLNAME,
                          doc.getPrefixedFullName(), context))
                  || ((action.equals("view") && doc.getFullName().equals("XWiki.AccountValidation"))))) {
```

But it's not taken into account in the REST API (or all resource reference handler which require an authenticated user) which means the user can pretty much do anything it wants (including enabling itself I think, unless there is a listener to protect that).

IMO, the user should be authenticated but should not be set as context user and instead be set in a special property storing the disabled user so that things related to disabled user can check it. That way, the access is safe by default (most of the code will see the context as not being authenticated) and only if you want to do something special with disabled user (like a process to be granted access again) you still have the info.

Reproduction steps:

- Create a user Foo and disable it
- Send following request with Foo authentication headers:

```
curl -X PUT -i 'http://localhost:8080/xwiki/rest/wikis/xwiki/spaces/XWiki/pages/Foo/objects/XWiki.XWikiUsers/0/properties/
```

- Login with Foo on the wiki

Expected result:

- Foo should still be disabled and the CURL request should not work

Obtained result:

- Foo is now enabled

Issue Links

causes

XWIKI-19645 Manual user account validation using a validation key does not succeed due to a NPE	CLOSED

is related to

XWIKI-19696 Disabled users can access and download attachments from wiki pages	CLOSED

XWIKI-12654 Add UI to activate/deactivate users CLOSED

links to

Github Security advisory

Activity

Newest first

Simon Urli added a comment - 31/Mar/22 17:20

Note that the fix provided with this issue is backed by the test added in https://github.com/xwiki/xwiki-platform/commit/1cb8750c1a54f76c0991d1634da9381252f3e89d.
This test was not added with the same key to avoid a too obvious disclosure of the reproduction steps.

Simon Urli added a comment - 25/Mar/22 10:36 - edited

> IMO, the user should be authenticated but should not be set as context user and instead be set in a special property storing the disabled user so that things related to disabled user can check it.

So I applied this idea in my fix, note that there's a few change in the behaviour related to it: mainly it means that on a close wiki, logging-in with an inactive user won't show anymore the navigation and everything. Since the context user is guest, the wiki is not really accessed. Now I kept the capability to use the allowedPage property: the difference is that the user needs the actual link to that page, since he cannot access it through navigation.

Also I had to modify a bit the drawer template, to display the logout link when a inactive user logged in: with the previous template it wasn't possible since the context user is guest in such case now.

Simon Urli added a comment - 24/Mar/22 14:11

So this issue impacts all inactive users: AFAICS the boolean the check for inactive users is as old as 1.1M3 and maybe older than that (I tracked it down until ~~XWIKI-12~~). Now this issue has been made more important recently in 11.3RC1 with ~~XWIKI-12654~~ and the capability to easily disable users.

Simon Urli added a comment - 24/Mar/22 11:11

Note that there is a configuration to handle for this, which is: https://www.xwiki.org/xwiki/bin/view/Documentation/AdminGuide/Configuration/#HAllowedPagesforInactiveUsers but AFAICS right now this is not supported for users who have been disabled. It's only supported for users not yet activated. IMO we should keep this behaviour and fix the doc.

People

Assignee:

Simon Urli

Reporter:

Thomas Mortagne

Votes:

0 Vote for this issue

Watchers:

2 Start watching this issue

Dates

Created:

23/Mar/22 18:01

Updated:

08/Sep/22 14:34

Resolved:

31/Mar/22 17:23

Date of First Response:

24/Mar/22 11:11 AM