phpcmsV9.5.8 后台两个低权限拿shell

potato / 2017-04-14 14:40:44 / 浏览数 3952 安全技术 漏洞分析 顶(0) 踩(0)

本文也是分析t00ls表哥的文章后，无意中发现的另一处代码执行漏洞。版本是phpcms v9.5.8 现在官方已经修复了。

poc

根据poc代码所在的url连接，我们可以定位到是phpcms/modules/content/content.php文件中的public_categorys函数，

这段代码是在构造categorys数组，并为下面的操作做准备

从这段代码中可以看出，如果$categorys不为空，则进入if条件语句中，在这里switch语句中，$from无论是什么值，$strs将会一定存在$_GET['menuid']这个变量的值。并

上面的是这个函数的介绍，下面是这个函数所存在漏洞的地方

```
            if($this->get_child($id)){
eval("\$nstr = \"$str2\";");
$this->str .= $nstr;
if($showlevel == 0 || ($showlevel > 0 && $showlevel > $currentlevel)) {
$this->get_treeview($id, $effected_id, $str, $str2, $showlevel, $style, $currentlevel+1, TRUE);
} elseif($showlevel > 0 && $showlevel == $currentlevel) {
$this->str .= $placeholder;
}
} else {
eval("\$nstr = \"$str\";");
$this->str .= $nstr;
}
```

在这里，首先判断一下是不是子样式表，如果不是将会通过eval去执行$str2，如果是子样式表，则会执行$str，也就是一定会执行包含恶意代码的字符串。

漏洞修复方案

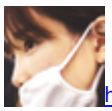
- 及时升级phpcms最近版本即可
- 如果无法升级，可以在phpcms/modules/content/content.php中的public_categorys和public_sub_categorys这两个函数的第一行加入下列代码

```
$_GET['menuid'] = intval($_GET['menuid']);
```

即可修复漏洞

上一篇：Cobalt Strike搭建和使... 下一篇：Phpcms_V9任意文件上传 漏洞分析

1. 1 条回复


hades 2017-04-14 15:09:50

稳 欢迎多多探讨

0 回复Ta