Yunus Şahin Follow

Mar 15, 2021 · 1 min read · Listen

Save

TP-Link’s TL-WPA4220 V4.0 Cleartext Credentials in Cookie

Model: TL-WPA4220

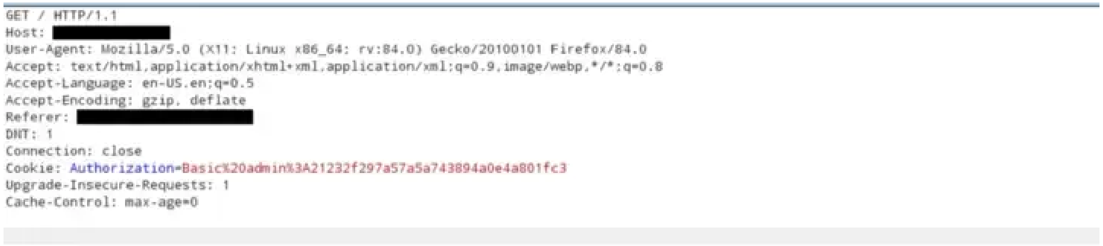
Firmware: 4.0.2 Build 20180308 Rel.37064

Hardware: Version: TL-WPA4220 v4.0

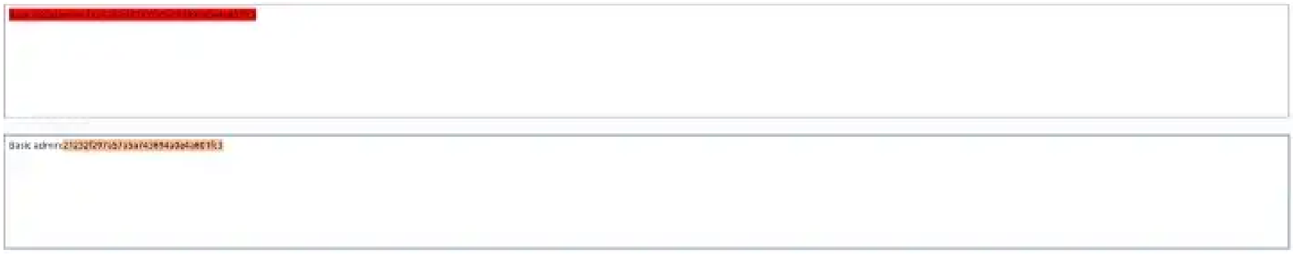
CVE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28857

Update: https://static.tp-link.com/beta/2021/202103/20210316/wpa4220v3_eu-up-ver1-0-0-P1-20210316-rel53466-APPLC.zip

TP-Link’s TL-WPA4220 V4.0 username and password are sent via the cookie.



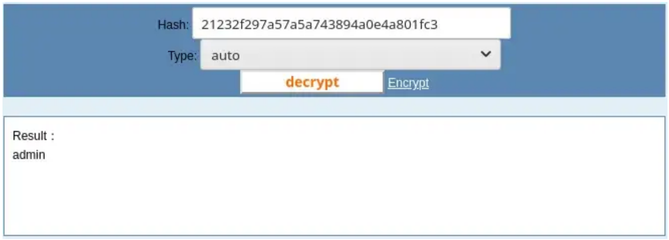
```
GET / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: [redacted]
DNT: 1
Connection: close
Cookie: Authorization=Basic%20admin%3A21232f297a57a5a743894a0e4a801fc3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



```
[illegible]
```

```
Basic admin:21232f297a57a5a743894a0e4a801fc3
```

The password is sent as md5.



Hash: 21232f297a57a5a743894a0e4a801fc3

Type: auto

Result :
admin

If an attacker cracks the md5, attacker may log in existing router interface.