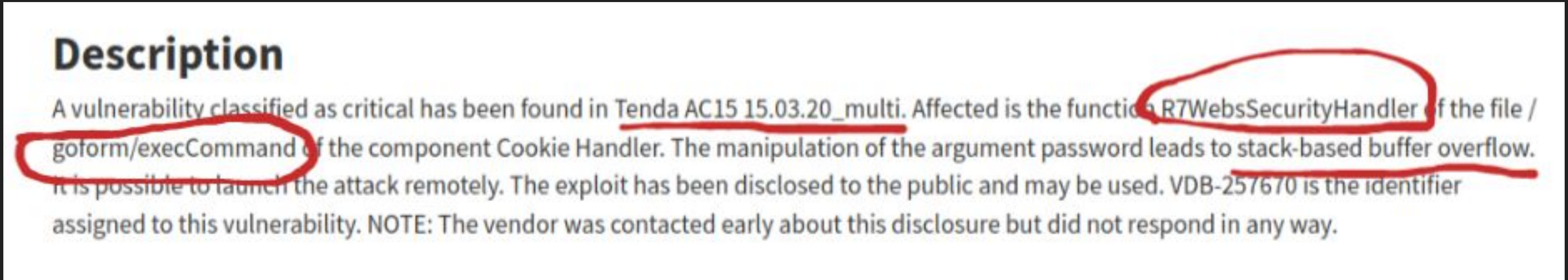
Time Travel Analysis VS Debuggers

Pierre Mondon and Yoan Lefevre
Security analysts @eshard

An illustrated example through CVE-2024-2815

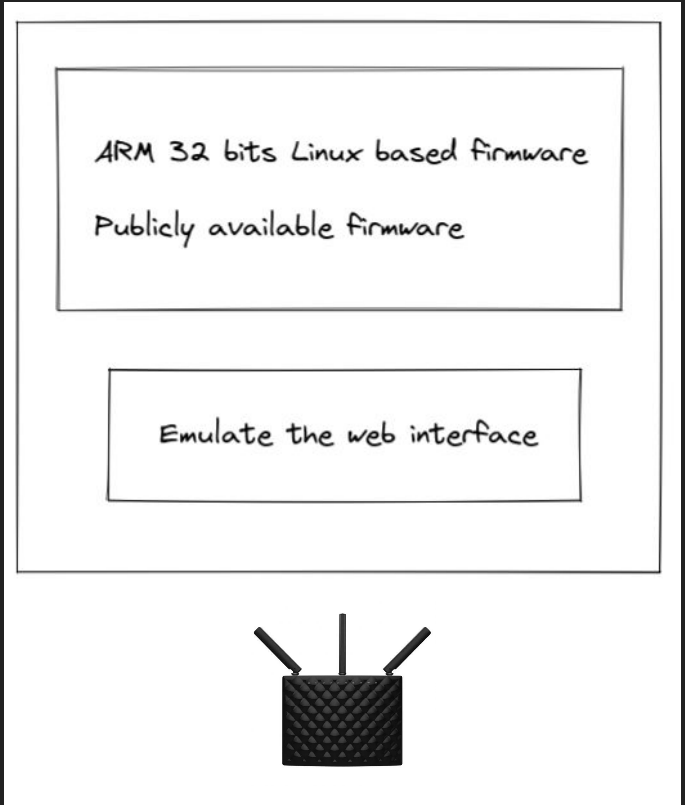
Tenda AC15 router web interface



Description

A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

Reproduce and analyse the vulnerability

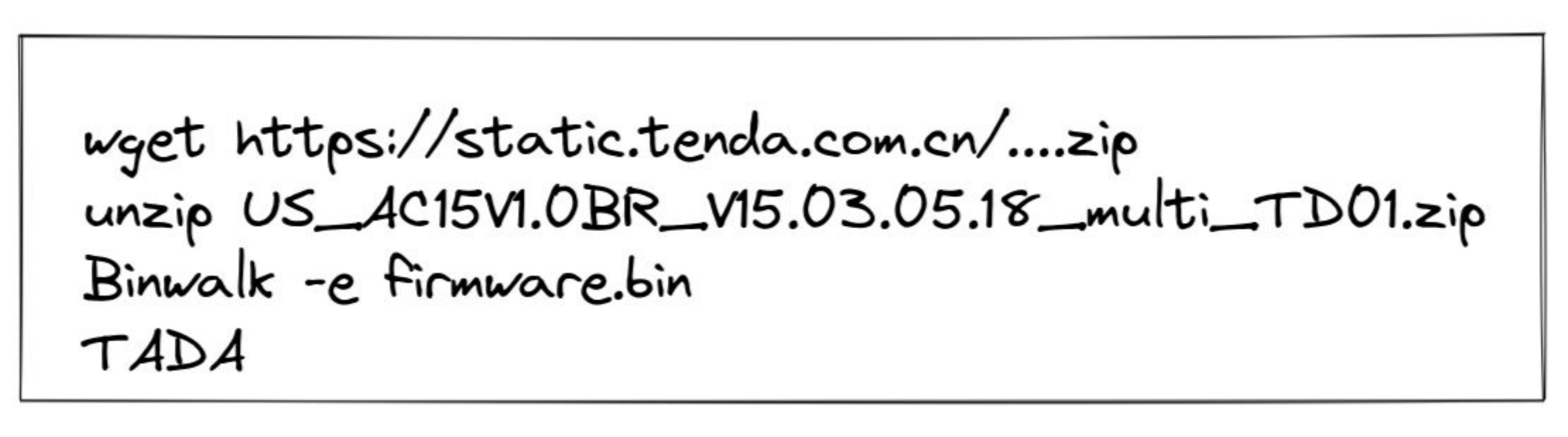


ARM 32 bits Linux based firmware

Publicly available firmware

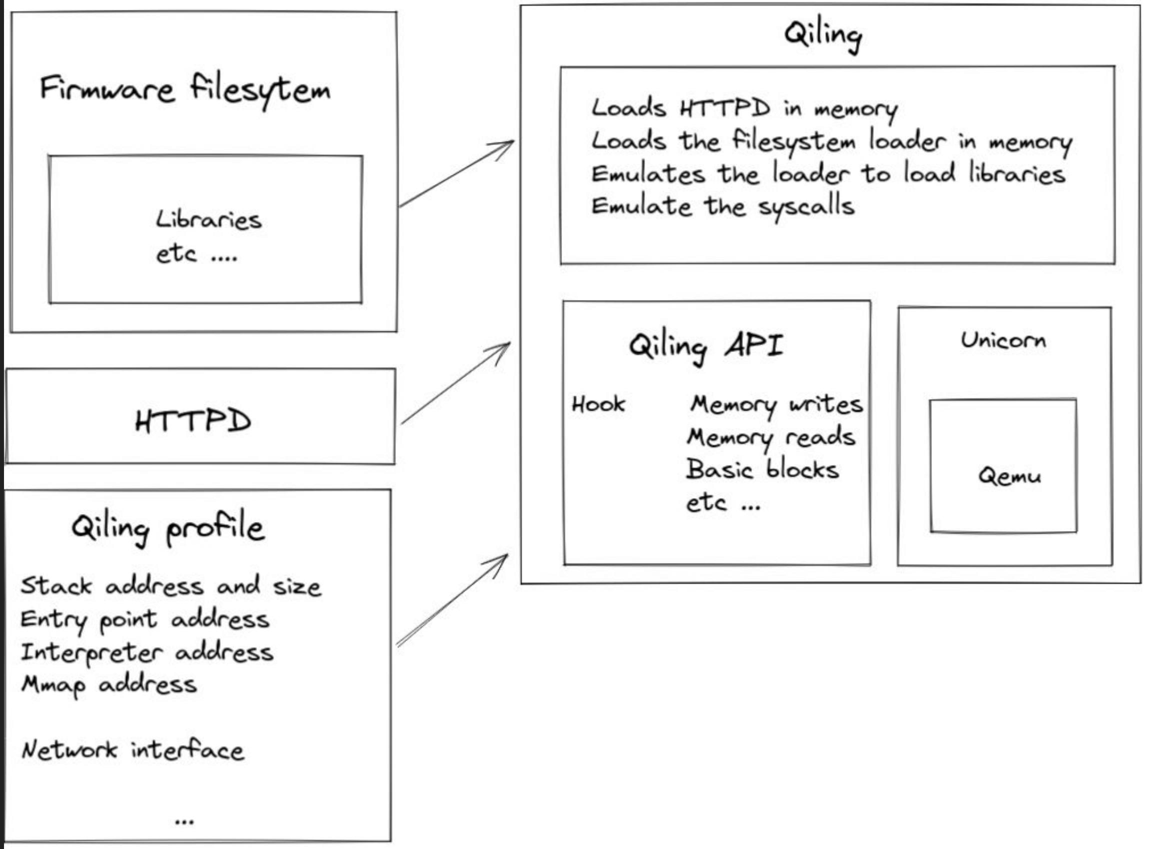
Emulate the web interface

Firmware extraction (very hard !!!)



```
wget https://static.tenda.com.cn/....zip
unzip US_AC15V1.0BR_V15.03.05.18_multi_TD01.zip
Binwalk -e firmware.bin
TADA
```

Firmware emulation



Firmware filesytem

Libraries
etc ....

HTTPD

Qiling profile

Stack address and size
Entry point address
Interpreter address
Mmap address

Network interface

...

Qiling

Loads HTTPD in memory
Loads the filesystem loader in memory
Emulates the loader to load libraries
Emulate the syscalls

Qiling API

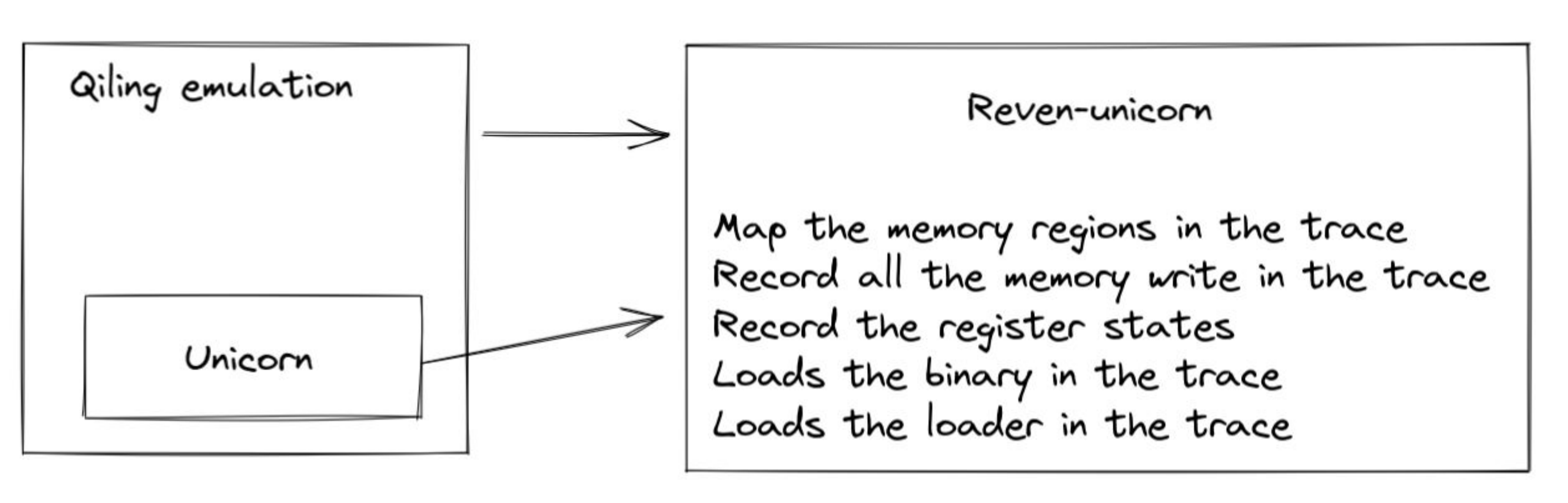
Hook

Memory writes
Memory reads
Basic blocks
etc ...

Unicorn

Qemu

Record the emulation for time travel analysis



Qiling emulation

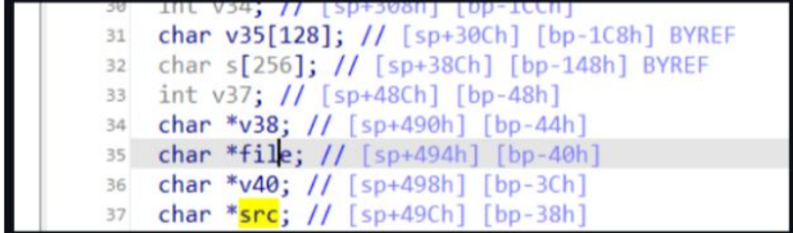
Unicorn

Reven-unicorn

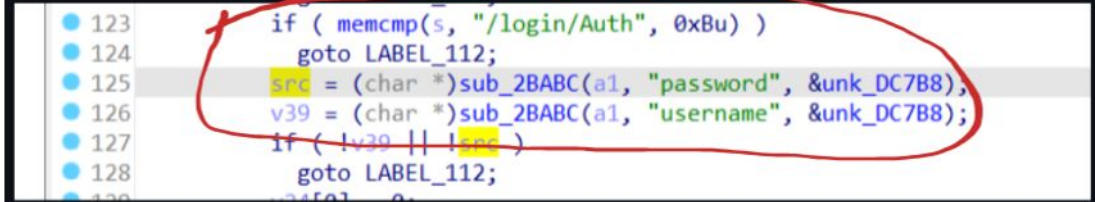
Map the memory regions in the trace
Record all the memory write in the trace
Record the register states
Loads the binary in the trace
Loads the loader in the trace

Vulnerability details

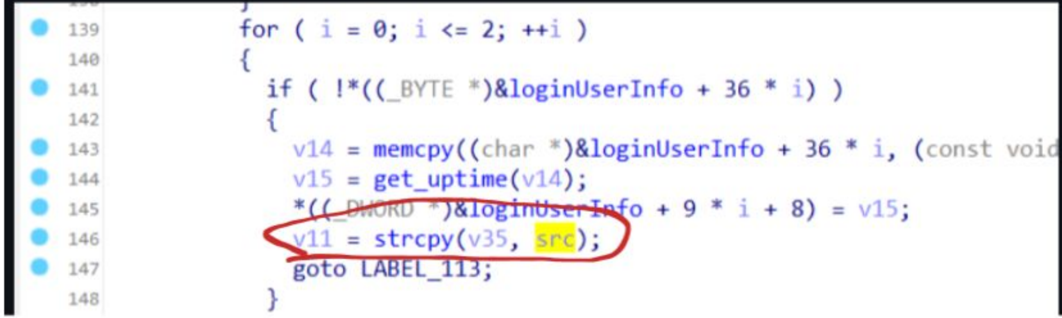
The Tenda AC15 V15.03.05.18 firmware has a stack overflow vulnerability in the `R7WebsSecurityHandler` function. The `src` variable receives the `password` parameter from a POST request and is later assigned to the `v35` variable, which is fixed at 128 bytes. However, since the user can control the input of `password`, the statement `strcpy(v35, src);` can cause a buffer overflow. The user-provided `password` can exceed the capacity of the `v35` array, triggering this security vulnerability.



```
int v34; // [sp+308h] [bp-1CCh]
char v35[128]; // [sp+30Ch] [bp-1C8h] BYREF
char s[256]; // [sp+38Ch] [bp-148h] BYREF
int v37; // [sp+48Ch] [bp-48h]
char *v38; // [sp+490h] [bp-44h]
char *file; // [sp+494h] [bp-40h]
char *v40; // [sp+498h] [bp-3Ch]
char *src; // [sp+49Ch] [bp-38h]
```

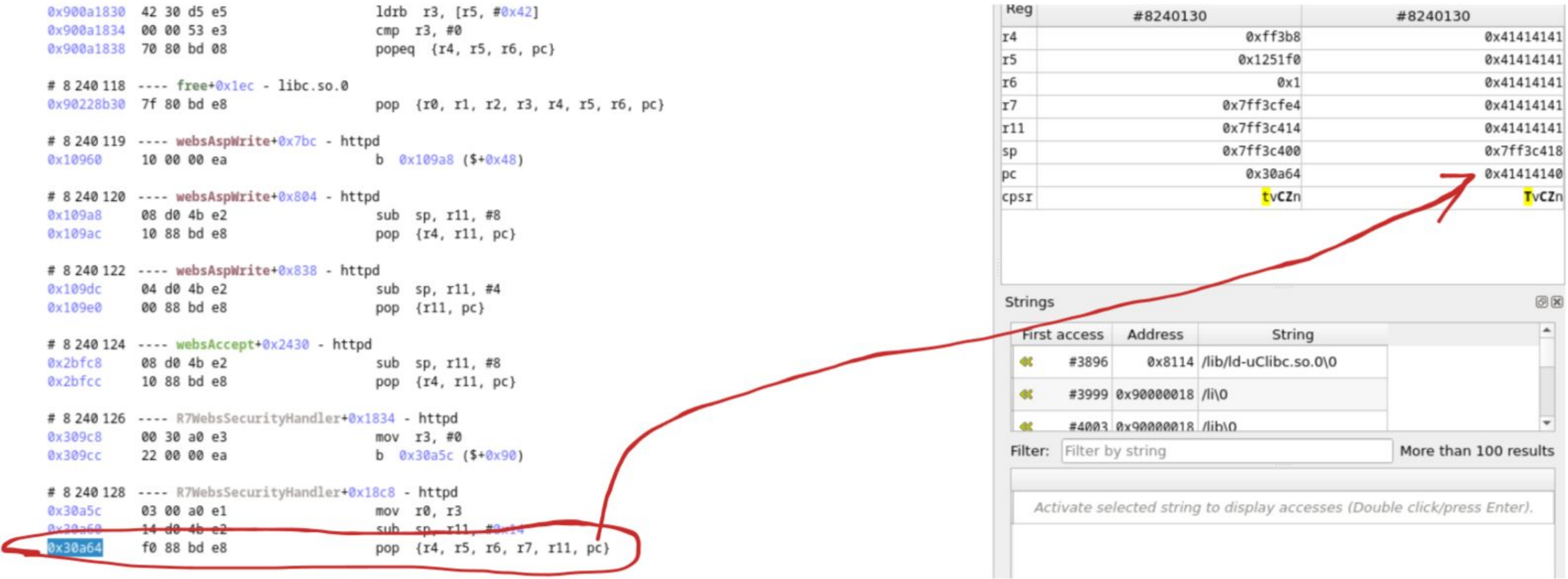


```
      if ( memcmp(s, "/login/Auth", 0xBu) )
        goto LABEL_112;
      src = (char *)sub_2BABC(a1, "password", &unk_DC7B8);
      v39 = (char *)sub_2BABC(a1, "username", &unk_DC7B8);
      if ( !v39 || !src )
        goto LABEL_112;
```



```
        for ( i = 0; i <= 2; ++i )
        {
          if ( !*((_BYTE *)&loginUserInfo + 36 * i) )
          {
            v14 = memcpy((char *)&loginUserInfo + 36 * i, (const void
            v15 = get_uptime(v14);
            *((_DWORD *)&loginUserInfo + 9 * i + 8) = v15;
            v11 = strcpy(v35, src);
            goto LABEL_113;
          }
```

Inside of the time travel view



```
0x900a1830  42 30 d5 e5          ldrb  r3, [r5, #0x42]
0x900a1834  00 00 53 e3          cmp  r3, #0
0x900a1838  70 80 bd 08          popeq  {r4, r5, r6, pc}

# 8 240 118 ---- free+0x1ec - libc.so.0
0x90228b30  7f 80 bd e8          pop  {r0, r1, r2, r3, r4, r5, r6, pc}

# 8 240 119 ---- websAspWrite+0x7bc - httpd
0x10960     10 00 00 ea          b  0x109a8 ($+0x48)

# 8 240 120 ---- websAspWrite+0x804 - httpd
0x109a8     08 d0 4b e2          sub  sp, r11, #8
0x109ac     10 88 bd e8          pop  {r4, r11, pc}

# 8 240 122 ---- websAspWrite+0x838 - httpd
0x109dc     04 d0 4b e2          sub  sp, r11, #4
0x109e0     00 88 bd e8          pop  {r11, pc}

# 8 240 124 ---- websAccept+0x2430 - httpd
0x2bfc8     08 d0 4b e2          sub  sp, r11, #8
0x2bfcc     10 88 bd e8          pop  {r4, r11, pc}

# 8 240 126 ---- R7WebsSecurityHandler+0x1834 - httpd
0x309c8     00 30 a0 e3          mov  r3, #0
0x309cc     22 00 00 ea          b  0x30a5c ($+0x90)

# 8 240 128 ---- R7WebsSecurityHandler+0x18c8 - httpd
0x30a5c     03 00 a0 e1          mov  r0, r3
0x30a60     14 d0 4b e2          sub  sp, r11, #0x14
0x30a64     f0 88 bd e8          pop  {r4, r5, r6, r7, r11, pc}
```

Reg	#8240130	#8240130
r4	0xff3b8	0x41414141
r5	0x1251f0	0x41414141
r6	0x1	0x41414141
r7	0x7ff3cfe4	0x41414141
r11	0x7ff3c414	0x41414141
sp	0x7ff3c400	0x7ff3c418
pc	0x30a64	0x41414140
cpsr	tvCZn	TvCZn

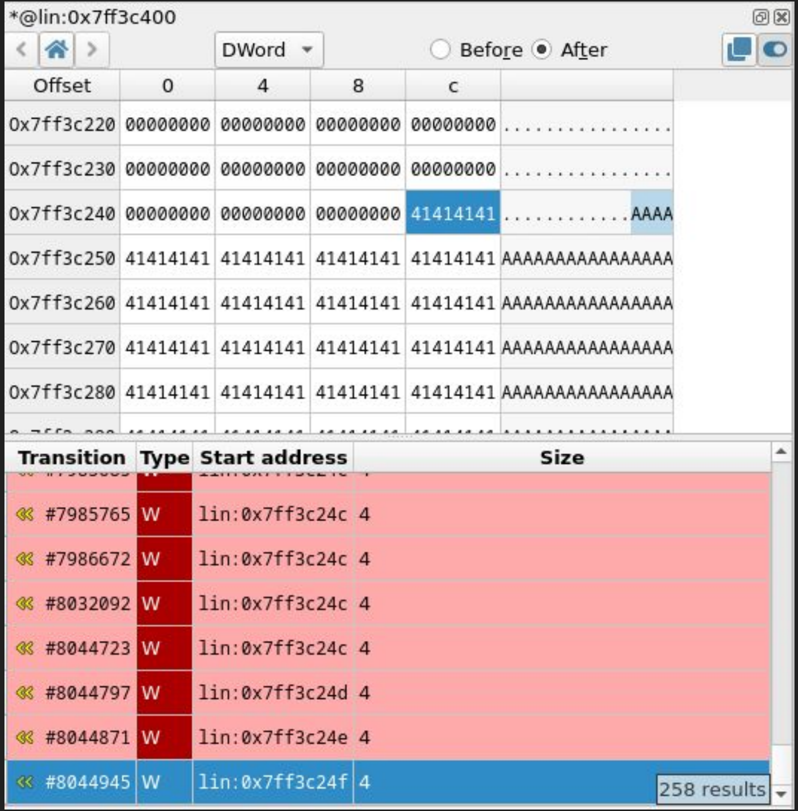
Strings

First access	Address	String
#3896	0x8114	/lib/ld-uClibc.so.0\0
#3999	0x90000018	/li\0
#4003	0x90000018	/lib\0

Filter: Filter by string   More than 100 results

Activate selected string to display accesses (Double click/press Enter).

Inside of the time travel view



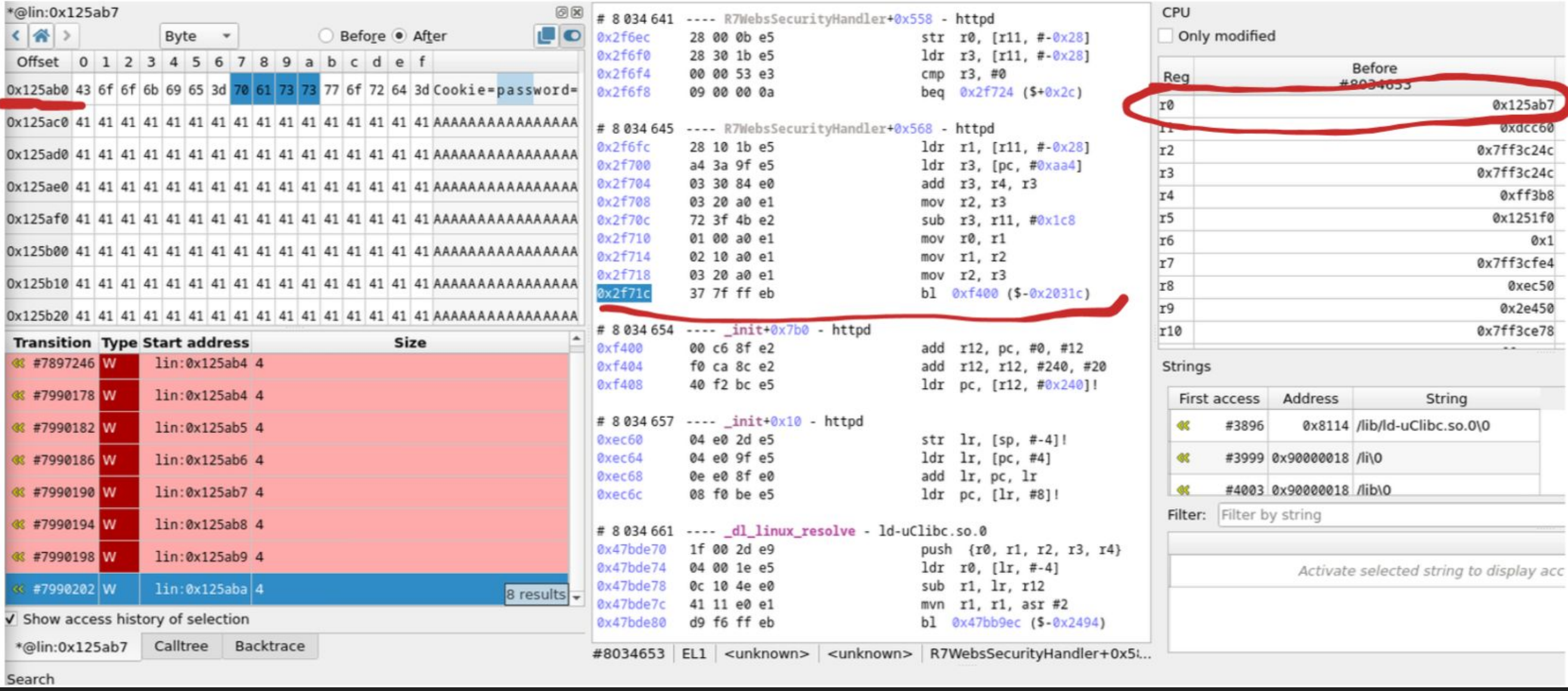
*@lin:0x7ff3c400

```
Offset      0        4        8        c
0x7ff3c220 00000000 00000000 00000000 00000000 ................
0x7ff3c230 00000000 00000000 00000000 00000000 ................
0x7ff3c240 00000000 00000000 00000000 41414141 ............AAAA
0x7ff3c250 41414141 41414141 41414141 41414141 AAAAAAAAAAAAAAAA
0x7ff3c260 41414141 41414141 41414141 41414141 AAAAAAAAAAAAAAAA
0x7ff3c270 41414141 41414141 41414141 41414141 AAAAAAAAAAAAAAAA
0x7ff3c280 41414141 41414141 41414141 41414141 AAAAAAAAAAAAAAAA
```

Transition	Type	Start address	Size
« #7985765	W	lin:0x7ff3c24c	4
« #7986672	W	lin:0x7ff3c24c	4
« #8032092	W	lin:0x7ff3c24c	4
« #8044723	W	lin:0x7ff3c24c	4
« #8044797	W	lin:0x7ff3c24d	4
« #8044871	W	lin:0x7ff3c24e	4
« #8044945	W	lin:0x7ff3c24f	4

258 results

Inside of the time travel view



```
Offset   0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
0x125ab0 43 6f 6f 6b 69 65 3d 70 61 73 73 77 6f 72 64 3d Cookie=password=
0x125ac0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125ad0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125ae0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125af0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125b00 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125b10 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
0x125b20 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
```

Transition	Type	Start address	Size
« #7897246	W	lin:0x125ab4	4
« #7990178	W	lin:0x125ab4	4
« #7990182	W	lin:0x125ab5	4
« #7990186	W	lin:0x125ab6	4
« #7990190	W	lin:0x125ab7	4
« #7990194	W	lin:0x125ab8	4
« #7990198	W	lin:0x125ab9	4
« #7990202	W	lin:0x125aba	4

```
# 8 034 641  ---- R7WebsSecurityHandler+0x558 - httpd
0x2f6ec     28 00 0b e5              str  r0, [r11, #-0x28]
0x2f6f0     28 30 1b e5              ldr  r3, [r11, #-0x28]
0x2f6f4     00 00 53 e3              cmp  r3, #0
0x2f6f8     09 00 00 0a              beq  0x2f724 ($+0x2c)

# 8 034 645  ---- R7WebsSecurityHandler+0x568 - httpd
0x2f6fc     28 10 1b e5              ldr  r1, [r11, #-0x28]
0x2f700     a4 3a 9f e5              ldr  r3, [pc, #0xaa4]
0x2f704     03 30 84 e0              add  r3, r4, r3
0x2f708     03 20 a0 e1              mov  r2, r3
0x2f70c     72 3f 4b e2              sub  r3, r11, #0x1c8
0x2f710     01 00 a0 e1              mov  r0, r1
0x2f714     02 10 a0 e1              mov  r1, r2
0x2f718     03 20 a0 e1              mov  r2, r3
0x2f71c     37 7f ff eb              bl  0xf400 ($-0x2031c)

# 8 034 654  ---- _init+0x7b0 - httpd
0xf400      00 c6 8f e2              add  r12, pc, #0, #12
0xf404      f0 ca 8c e2              add  r12, r12, #240, #20
0xf408      40 f2 bc e5              ldr  pc, [r12, #0x240]!

# 8 034 657  ---- _init+0x10 - httpd
0xec60      04 e0 2d e5              str  lr, [sp, #-4]!
0xec64      04 e0 9f e5              ldr  lr, [pc, #4]
0xec68      0e e0 8f e0              add  lr, pc, lr
0xec6c      08 f0 be e5              ldr  pc, [lr, #8]!

# 8 034 661  ---- _dl_linux_resolve - ld-uClibc.so.0
0x47bde70   1f 00 2d e9              push  {r0, r1, r2, r3, r4}
0x47bde74   04 00 1e e5              ldr  r0, [lr, #-4]
0x47bde78   0c 10 4e e0              sub  r1, lr, r12
0x47bde7c   41 11 e0 e1              mvn  r1, r1, asr #2
0x47bde80   d9 f6 ff eb              bl  0x47bb9ec ($-0x2494)
```

#8034653 | EL1 | <unknown> | <unknown> | R7WebsSecurityHandler+0x5...

CPU

□ Only modified

Reg	Before #8034653
r0	0x125ab7
r1	0xdcc60
r2	0x7ff3c24c
r3	0x7ff3c24c
r4	0xff3b8
r5	0x1251f0
r6	0x1
r7	0x7ff3cfe4
r8	0xec50
r9	0x2e450
r10	0x7ff3ce78

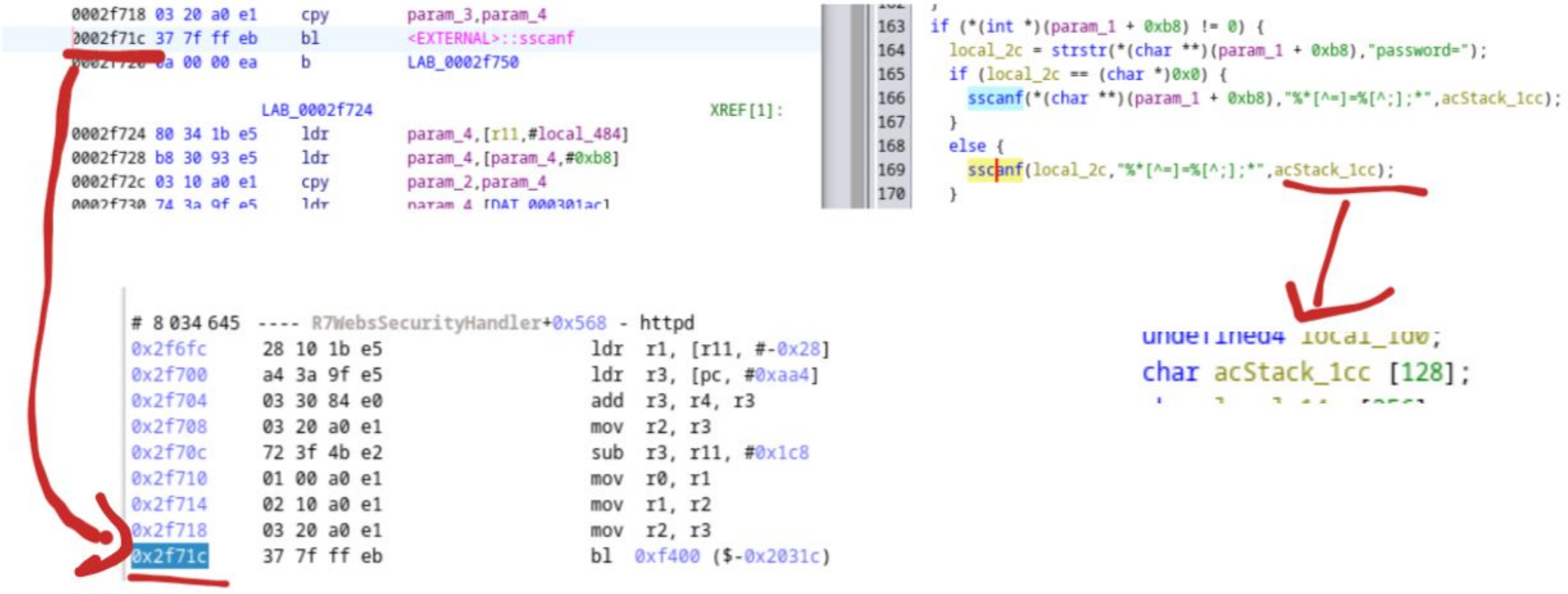
Strings

First access	Address	String
« #3896	0x8114	/lib/ld-uClibc.so.0\0
« #3999	0x90000018	/li\0
« #4003	0x90000018	/lib\0

Filter: Filter by string

Activate selected string to display acc

Inside Ghidra



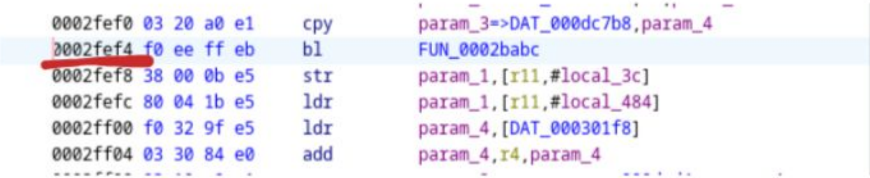
```
0002f718 03 20 a0 e1      cpy        param_3,param_4
0002f71c 37 7f ff eb      bl         <EXTERNAL>::sscanf
0002f720 0a 00 00 ea      b          LAB_0002f750

                  LAB_0002f724                                    XREF[1]:
0002f724 80 34 1b e5      ldr        param_4,[r11,#local_484]
0002f728 b8 30 93 e5      ldr        param_4,[param_4,#0xb8]
0002f72c 03 10 a0 e1      cpy        param_2,param_4
0002f730 74 3a 9f e5      ldr        param_4,[DAT_000301ac]
```

```
  if (*(int *)(param_1 + 0xb8) != 0) {
    local_2c = strstr(*(char **)(param_1 + 0xb8),"password=");
    if (local_2c == (char *)0x0) {
      sscanf(*(char **)(param_1 + 0xb8),"%*[^=]=%[^;];*",acStack_1cc);
    }
    else {
      sscanf(local_2c,"%*[^=]=%[^;];*",acStack_1cc);
    }
```

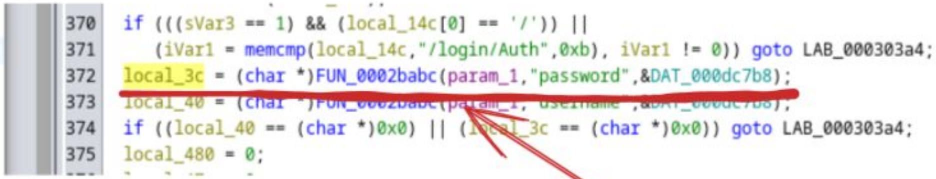
```
# 8 034 645  ---- R7WebsSecurityHandler+0x568 - httpd
0x2f6fc      28 10 1b e5                ldr  r1, [r11, #-0x28]
0x2f700      a4 3a 9f e5                ldr  r3, [pc, #0xaa4]
0x2f704      03 30 84 e0                add  r3, r4, r3
0x2f708      03 20 a0 e1                mov  r2, r3
0x2f70c      72 3f 4b e2                sub  r3, r11, #0x1c8
0x2f710      01 00 a0 e1                mov  r0, r1
0x2f714      02 10 a0 e1                mov  r1, r2
0x2f718      03 20 a0 e1                mov  r2, r3
0x2f71c      37 7f ff eb                bl  0xf400 ($-0x2031c)
```

```
undefined4 local_1d0;
char acStack_1cc [128];
```

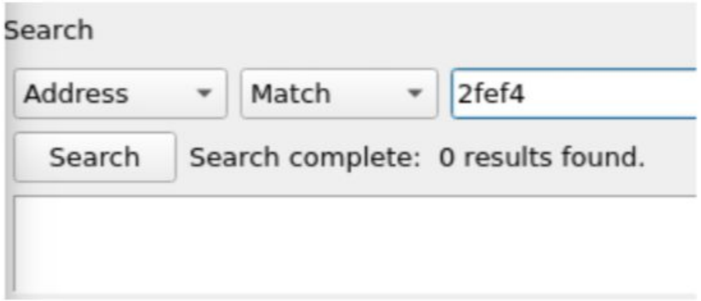
Quid du strcpy ?????



```
0002fef0 03 20 a0 e1    cpy     param_3=>DAT_000dc7b8,param_4
0002fef4 f0 ee ff eb    bl      FUN_0002babc
0002fef8 38 00 0b e5    str     param_1,[r11,#local_3c]
0002fefc 80 04 1b e5    ldr     param_1,[r11,#local_484]
0002ff00 f0 32 9f e5    ldr     param_4,[DAT_000301f8]
0002ff04 03 30 84 e0    add     param_4,r4,param_4
```



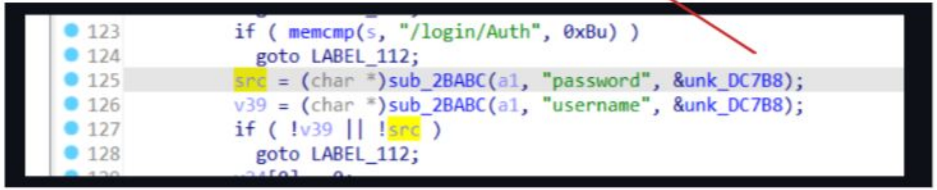
```
if (((sVar3 == 1) && (local_14c[0] == '/')) ||
   (iVar1 = memcmp(local_14c,"/login/Auth",0xb), iVar1 != 0)) goto LAB_000303a4;
local_3c = (char *)FUN_0002babc(param_1,"password",&DAT_000dc7b8);
~~local_40 = (char *)FUN_0002babc(param_1,"username",&DAT_000dc7b8);~~
if ((local_40 == (char *)0x0) || (local_3c == (char *)0x0)) goto LAB_000303a4;
local_480 = 0;
```



Search

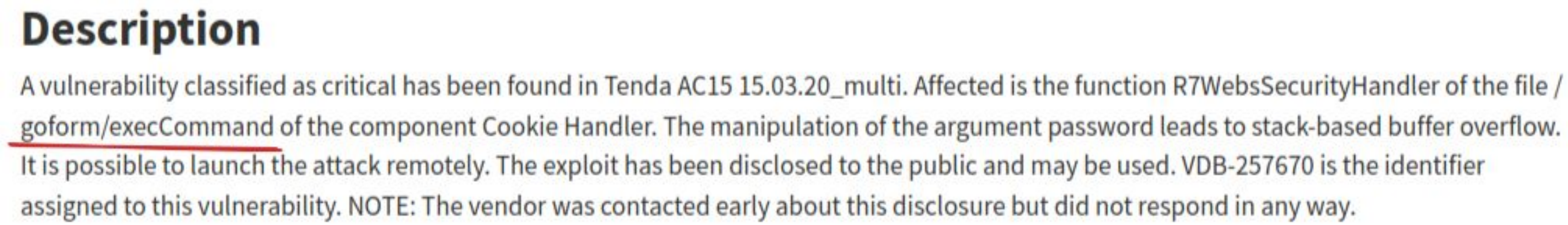
Address ▾ | Match ▾ | 2fef4

Search | Search complete: 0 results found.



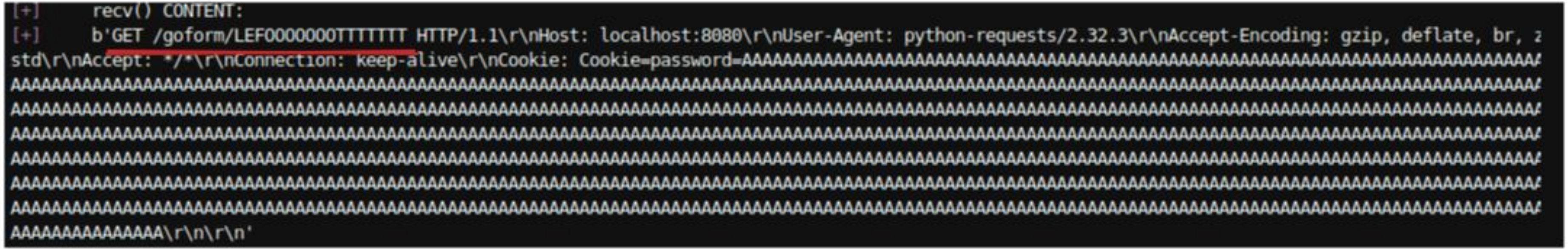
```
      if ( memcmp(s, "/login/Auth", 0xBu) )
        goto LABEL_112;
      src = (char *)sub_2BABC(a1, "password", &unk_DC7B8);
      v39 = (char *)sub_2BABC(a1, "username", &unk_DC7B8);
      if ( !v39 || !src )
        goto LABEL_112;
```

Quid du /goform/execCommand ????



Description

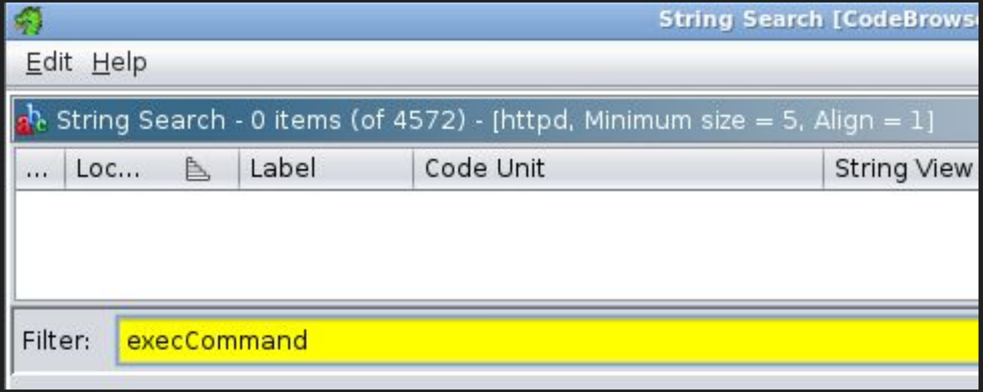
A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.



```
[+]     recv() CONTENT:
[+]     b'GET /goform/LEFOOOOOOOTTTTTTT HTTP/1.1\r\nHost: localhost:8080\r\nUser-Agent: python-requests/2.32.3\r\nAccept-Encoding: gzip, deflate, br, z
std\r\nAccept: */*\r\nConnection: keep-alive\r\nCookie: Cookie=password=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA\r\n\r\n'
```

/goform/nimportequoimemelefoot

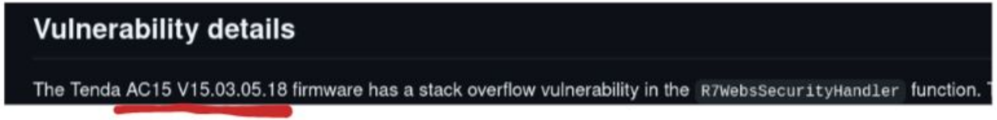
Fallback route



String Search - 0 items (of 4572) - [httpd, Minimum size = 5, Align = 1]

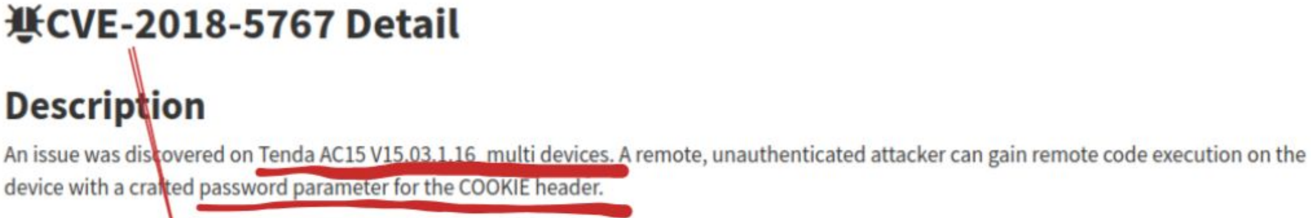
Filter: execCommand

CVE-2018-5767 ???



Vulnerability details

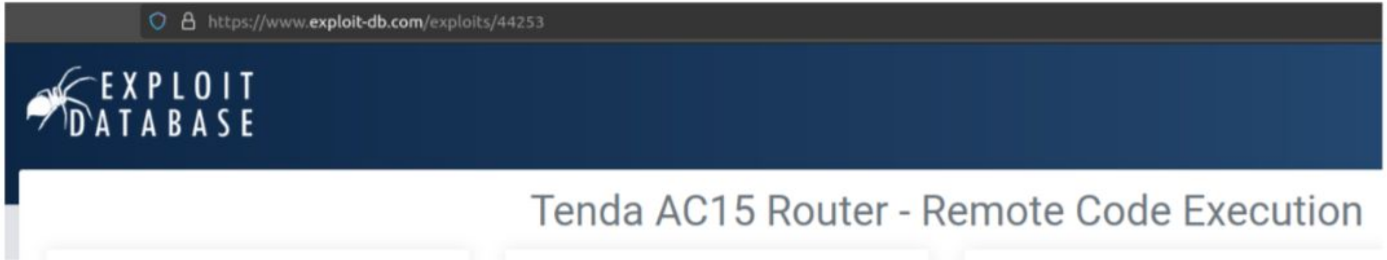
The Tenda AC15 V15.03.05.18 firmware has a stack overflow vulnerability in the `R7WebsSecurityHandler` function.



CVE-2018-5767 Detail

Description

An issue was discovered on Tenda AC15 V15.03.1.16 multi devices. A remote, unauthenticated attacker can gain remote code execution on the device with a crafted password parameter for the COOKIE header.



https://www.exploit-db.com/exploits/44253

Tenda AC15 Router - Remote Code Execution

Time Travel analysis VS Debugger

- We had access to the entire memory post-emulation
- Memory accesses history
- Easy to analyse the trace backward
- Code throughout time paradigm
- With Qiling you can still modify the runtime and record the modified runtime