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 cgitest.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

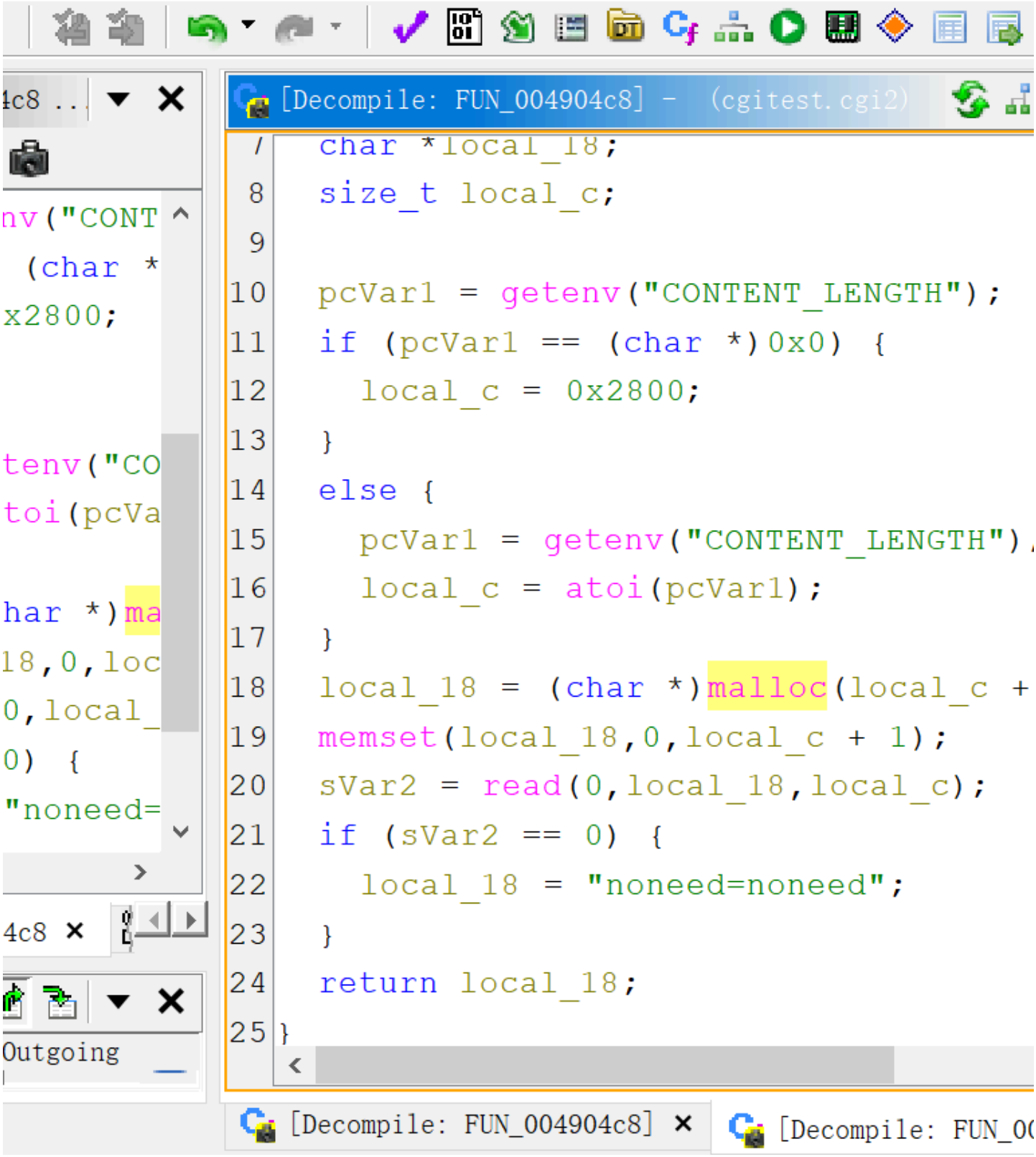
version: v2.1.40207

The firmware can be downloaded from this website. After extracting with binwalk, cgitest.cgi can be analyzed using QEMU with these commands:

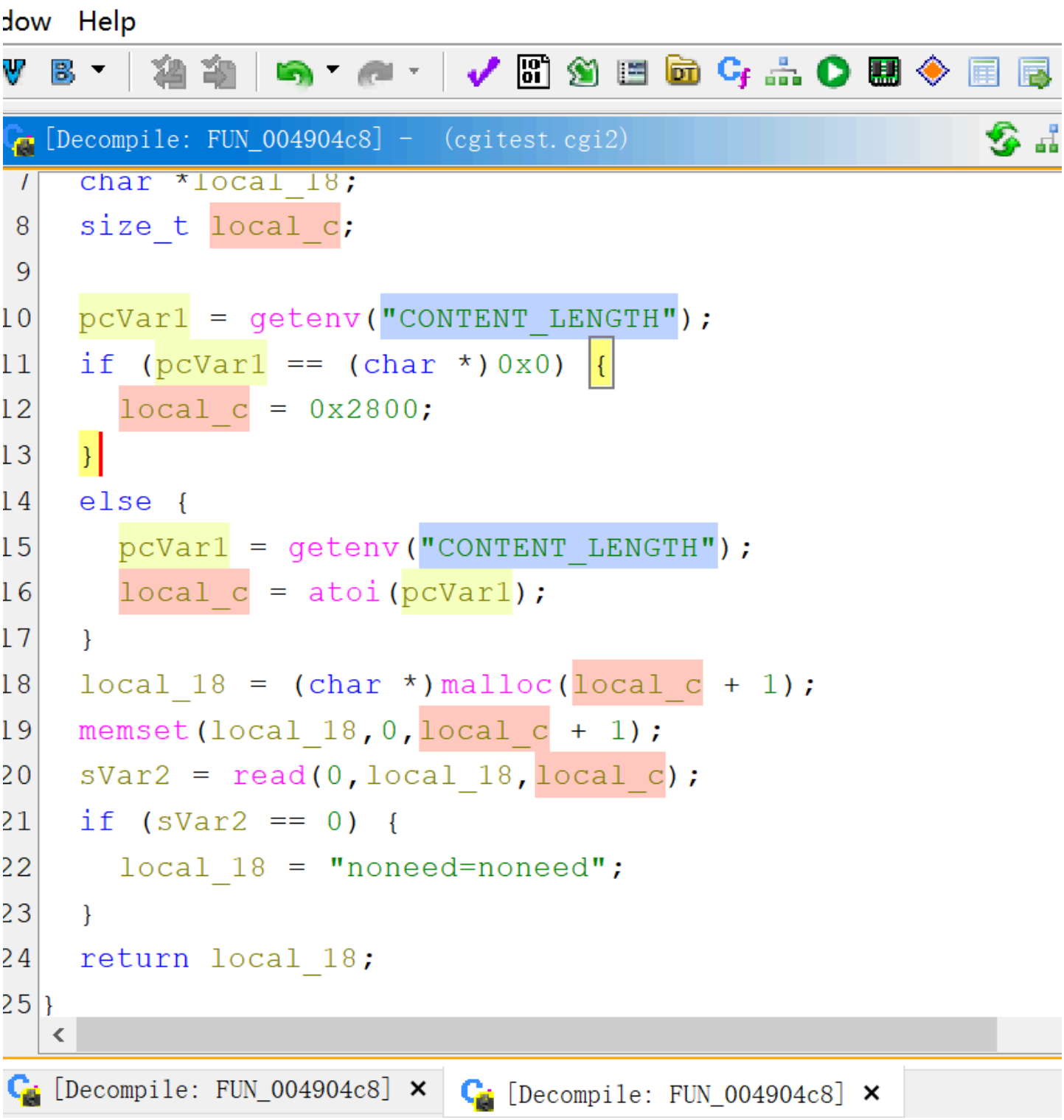
```
binwalk -Me netis-WF2880-V2.1.40207.bin
sudo chroot . ./qemu-mips-static ./bin/cgitest.cgi
```

analyze

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



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



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.