tenda overflow vulnerability

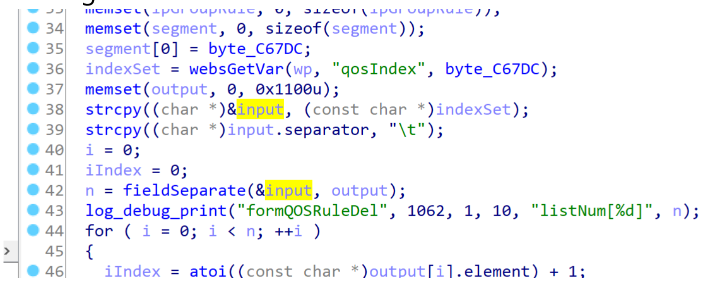
vendor:Tenda
product:G1,G3
version:V15.11.0.17(9502)_CN(G1),
V15.11.0.17(9502)_CN(G3)
type:Buffer Overflow
author:Jinwen Zhou、Yifeng Li、Yongjie Zheng;
institution:potatso@scnu、feng@scnu、eifiz@scnu

Vulnerability description

We found a buffer overflow vulnerability in Tenda Technology Tenda’s **G1 and G3** routers with firmware which was released recently，allows remote attackers to execute arbitrary code from a crafted GET request.

Buffer Overflow vulnerability

In **formQOSRuleDel** function, the parameter **“qosIndex”** is directly **strcpy** to a local variable placed on the stack, which overrides the return address of the function, causing buffer overflow.



```
memset(ipGroupRule, 0, sizeof(ipGroupRule));
memset(segment, 0, sizeof(segment));
segment[0] = byte_C67DC;
indexSet = websGetVar(wp, "qosIndex", byte_C67DC);
memset(output, 0, 0x1100u);
strcpy((char *)&input, (const char *)indexSet);
strcpy((char *)input.separator, "\t");
i = 0;
iIndex = 0;
n = fieldSeparate(&input, output);
log_debug_print("formQOSRuleDel", 1062, 1, 10, "listNum[%d]", n);
for ( i = 0; i < n; ++i )
{
  iIndex = atoi((const char *)output[i].element) + 1;
```

PoC

Buffer Overflow

We set the value of **qosIndex** as **aaaaaaaaaaaaaaaaaaaaaaaa......** and the router will cause buffer overflow.