

# Router Firmware Vulnerability Assessment Report

## (Hack2Hire )

|                           |   |
|---------------------------|---|
| 1. Firmware Name :        | <b>Damn Vulnerable Router Firmware (DVRF)</b> |
| 2. Firmware Compression : | gzip compressed                               |
| 3. Firmware File System:  | Squashfs Filesystem                           |
| 4. Firmware Kernel :      | Linux kernel version "2.6.22"                 |
| 5. Auditor Name :         | Manish Gupta                                  |

Detailed Report :

Vulnerability Name : Sensitive information

Risk Rating : Medium (CVSS : 6-7)

Sensitive Information:

These are the sensitive information which is contain in the given vulnerable firmware image.

1. Hidden File in Firmware : piggy file

2. Filesystem: squashfs

3. Linux Kernel Version : "2.6.22" (Out dated which contain main vulnerability )

4. Email : Ballardie@cs.ucl.ac.uk

5. Backdoor : pwnable directory

Step To Reproduce :

Step 1 : Extract the given Firmware Image (.bin file) using “Binwalk ” tool.

Terminal - root@kali: ~/Desktop/Hack2Hire/Challenge3

root@kali: ~/Desktop/Hack2Hire/Challenge3

Signatures:

DECIMAL

HEXADECIMAL

DESCRIPTION

0

0x0

BIN-Header, board ID: 1550, hardware version: 4702, firmware version: 1.0.0, build date: 2012-02-08

32

0x20

TRX firmware header, little endian, image size: 7753728 bytes, CRC32: 0x436822F6, flags: 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x192708, rootfs offset: 0x0

60

0x3C

gzip compressed data, maximum compression, has original file name: "piggy", from Unix, last modified: 2016-03-09 08:08:31

1648424

0x192728

Squashfs filesystem, little endian, non-standard signature, version 3.0, size: 6099215 bytes, 447 inodes, blocksize: 65536 bytes, created: 2016-03-10 04:34:22

Scan Time: 2018-09-02 11:17:01

Target File: /root/Desktop/Hack2Hire/Challenge3/\_EmbeddedFirmware.bin.extracted/piggy

MD5 Checksum: 1fab89cd8929471441d4130alc2cf477

Signatures: 344

DECIMAL

HEXADECIMAL

DESCRIPTION

3076096

0x2EF000

Linux kernel version "2.6.22 (root@localhost.localdomain)" (gcc version 4.2.3) #4 Wed Mar 9 02:05:36 CST 2016

3108912

0x2F7030

CRC32 polynomial table, little endian

3123228

0x2FA81C

CRC32 polynomial table, little endian

3422799

0x343A4F

Neighborly text, "NeighborSolicitsts"

3422823

0x343A67

Neighborly text, "NeighborAdvertisementsmp6OutDestUnreachs"

3423024

0x343B30

Neighborly text, "NeighborSolicitsirects"

3423052

0x343B4C

Neighborly text, "NeighborAdvertisementssponses"

3425755

0x3445DB

Neighborly text, "neighbor %2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x lost on port %d(%s)(%s)"

This Image Contain All the Sensitive information about the firmware image.

**Vulnerability Name :** Re-packing with malicious file

**Risk Rating :** Critical (CVSS : > 9)

### Backdoor Information:

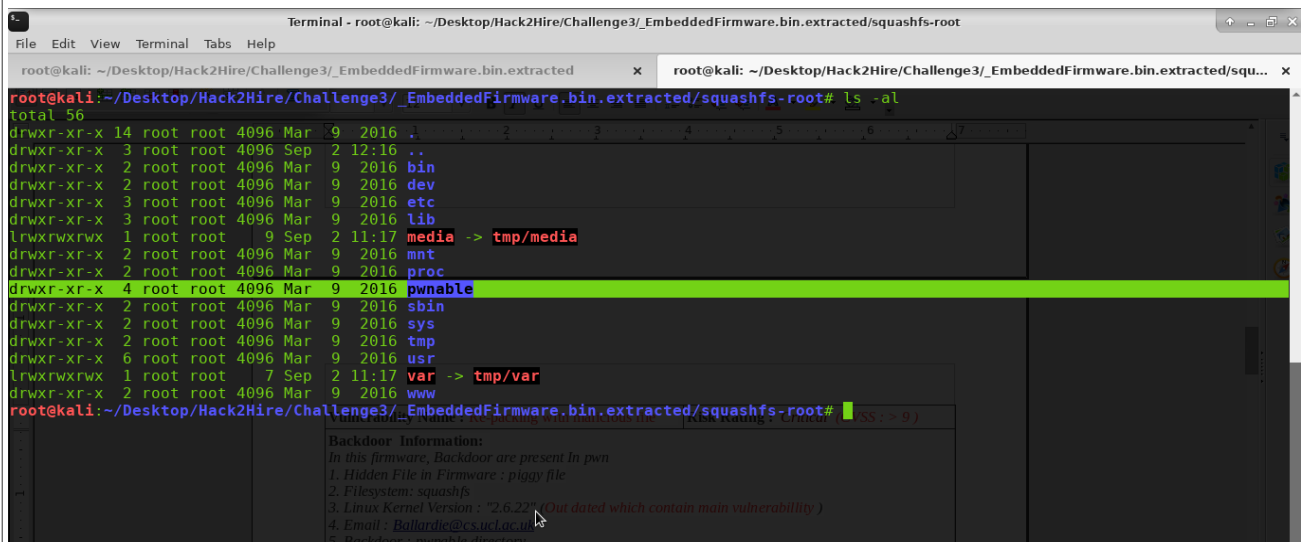
In this firmware, Backdoor are present In “pwnable”. Some of them vulnerable to buffer overflow attack. Attacker Re-packing these backdoor in this firmware image.

File Contain in “pwnable” Directory :

1. Intro directory
2. ShellCode\_Required directory

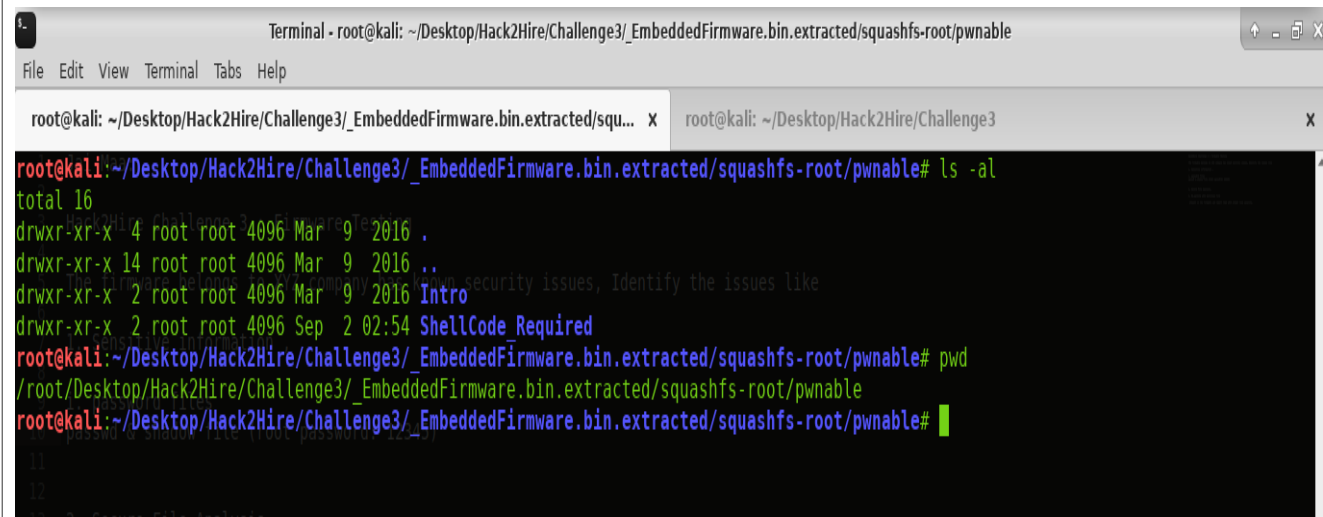
### Step To Reproduce :

Step 1 : Extract the given Firmware Image (.bin file) using “Binwalk” tool and show the list of file and directory in “squashfs-root” directory.



```
Terminal - root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root# ls -al
total 56
drwxr-xr-x 14 root root 4096 Mar  9 2016 .
drwxr-xr-x  3 root root 4096 Sep  2 12:16 ..
drwxr-xr-x  2 root root 4096 Mar  9 2016 bin
drwxr-xr-x  2 root root 4096 Mar  9 2016 dev
drwxr-xr-x  3 root root 4096 Mar  9 2016 etc
drwxr-xr-x  3 root root 4096 Mar  9 2016 lib
lrwxrwxrwx  1 root root    9 Sep  2 11:17 media -> tmp/media
drwxr-xr-x  2 root root 4096 Mar  9 2016 mnt
drwxr-xr-x  2 root root 4096 Mar  9 2016 proc
drwxr-xr-x  4 root root 4096 Mar  9 2016 pwnable
drwxr-xr-x  2 root root 4096 Mar  9 2016 sbin
drwxr-xr-x  2 root root 4096 Mar  9 2016 sys
drwxr-xr-x  2 root root 4096 Mar  9 2016 tmp
drwxr-xr-x  6 root root 4096 Mar  9 2016 usr
lrwxrwxrwx  1 root root    7 Sep  2 11:17 var -> tmp/var
drwxr-xr-x  2 root root 4096 Mar  9 2016 www
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root#
```

Step 2: Now show the list of files and directories in “pwnable” directory.



```
Terminal - root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable# ls -al
total 16
drwxr-xr-x  4 root root 4096 Mar  9 2016 .
drwxr-xr-x 14 root root 4096 Mar  9 2016 ..
drwxr-xr-x  2 root root 4096 Mar  9 2016 Intro
drwxr-xr-x  2 root root 4096 Sep  2 02:54 ShellCode_Required
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable# pwd
/root/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable#
```

Step 3: Now Backdoor file is there as shown below.

```
Terminal - root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable/Intro
File Edit View Terminal Tabs Help

root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable/Intro# ls
heap_overflow_01 README stack_bof_01 uaf_01
root@kali: ~/Desktop/Hack2Hire/Challenge3/_EmbeddedFirmware.bin.extracted/squashfs-root/pwnable/Intro# cat README
4
5 The firmware belongs to XYZ company has known security issues, Identify the issues like
6
7 1. Sensitive information ,
8
9 1. password file
10 passwd & shadow file (root password: 12345)
11
12
13 2. Secure File Analysis ,
14
15 3. Re-packing with malicious file
16
17 present in the firmware and report them with proper risk severity.
18
19 #####
20
21 Congrats! If you're reading this then you either connected to the E1550's UART or you extracted the binary with binwalk. Anyways, these
22 pwnables are for teaching you how to exploit other CPU architectures and in this case it's MIPS32 (Little Endian). The following files
23 are on here:
24
25 - stack_bof_01 - This is your run of the mill Buffer Overflow. This DOES NOT require shellcode to win, there is a function compiled into
26 the binary that is impossible to reach to normally. Your goal is to reach that function which will display a congrats message and execute
27 /bin/sh.
28
29 - heap_overflow_01 - This is just a basic heap overflow exercise. Just like the buffer overflow exercise there is a function that cannot
30 be reached normally and will require memory corruption in order to reach the function which will display a congrats message and execute
31 /bin/sh.
```

**It clearly shown here that attacker re-packing this firmware and add his own malicious code .**

**Thank You**