闻观行 赵振江

破解拉卡拉云POS机

设备详情

- 设备：拉卡拉云POS (APOS A8)
- 系统：Android 5.1.1
- APK网络校验、屏蔽开发者选项、拆机自毁
- 分区写保护、密码键盘清空键值

应用植入

- 蓝牙传入APK
  - 代理劫持服务器回包
  - {errorMessage: xxxx errorCode: 0000}

开启ADB

- am start -n com.android.settings/.DevelopmentSettings

绕过SYSTEM分区保护

```
int __fastcall android::SysmgrService::ISyssetFinished_ext(android::SysmgrService *this, int a2)
{
  unsigned int v2; // r4@1
  int result; // r0@3

  v2 = a2;
  _android_log_print(4, 0, "ISyssetFinished_ext=%d\n", a2, this, a2);
  if ( system_remount(0) )
    return 143;
  if ( v2 > 3 )
    return -1;
  result = sysdata_printf(20, "FINISHED_PRODUCT", 420, "%d", v2);
  if ( result >= 0 )
  {
    sysdata_update(20);
    if ( system_remount(1) )
      result = 143;
    else
      result = 0;
  }
  return result;
}
```

取得ROOT权限写文件能力

```
    case 21u:
      v8 = *(int (__fastcall **)(android::BnSysmgrHelper *))(*(_DWORD *)this + 96);
LABEL_28:
      v10 = v8(this);
LABEL_29:
      v16 = v10;
      v15 = v5;
      goto LABEL_30;
    case 22u:
      v25 = android::Parcel::readInt32(a3);
      v26 = v25;
      if ( v25 <= 0 )
        goto LABEL_12;
      v27 = malloc(v25 + 1);
      v14 = v27;
      if ( !v27 )
        goto LABEL_12;
      memset(v27, 0, v26 + 1);
      android::Parcel::read(v7, v14, v26);
      v17 = *(int (__fastcall **)(android::BnSysmgrHelper *, void *))(*(_DWORD *)v6 + 100);
      goto LABEL_39;
```

```
while ( index != 256 );
if ( !strncmp(str, "storagename=", 0xCu) )
{
  _sprintf_chk(storagename, 0, 256, "%s", &s[12]);
  _android_log_print(4, 0, "sysmgrhelper: storagename=%s\n", (int)storagename);
  v15 = 1;
}
if ( !strncmp(str, "storagepath=", 0xCu) )
{
  _sprintf_chk(storagepath, 0, 256, "%s", &s[12]);
  v4 = 1;
  _android_log_print(4, 0, "sysmgrhelper: storagepath=%s\n", (int)storagepath);
}
if ( !strncmp(str, "right=", 6u) )
{
  sscanf(&s[6], "%o", &right);
  _android_log_print(4, 0, "sysmgrhelper: right=%o\n", right);
}
if ( !strncmp(str, "deleteheadflg=", 0xEu) )
{
  sscanf(&s[14], "%d", &deleteheadflg);
  _android_log_print(4, 0, "sysmgrhelper: deleteheadflg=%d\n", deleteheadflg);
}
if ( !strncmp(str, "[specialfiledata]", 0x11u) )
  break;
memset(s, 0, 0x100u);
memset(str, 0, 0x100u);
}
if ( !v15 )
  goto LABEL_41;
if ( !v4 )
  goto LABEL_41;
memset(filename, 0, 0x200u);
_sprintf_chk(filename, 0, 512, "%s%s", storagepath, storagename);
_android_log_print(4, 0, "sysmgrhelper: copy, filepath=%s\n", (int)filename);
```

取得ROOT代码执行能力

- 写入/var/.download/exp到/sys/kernel/uevent_helper
  - 触发热插拔
  - u:r:kernel:s0

绕过虚拟键盘保护 截取刷卡口令

```
if ( pinKeyCode >= '0' )
{
  v5 = pThis->inputedPinLen;
  if ( pThis->maxPinLen > v5 )
  {
    pThis->clrPinBuf[v5] = pinKeyCode;
    v11 = (unsigned __int8)(v5 + 1);
    pThis->inputedPinLen = v11;
    memcpy(&clrPin_25988, pThis->clrPinBuf, v11);
    v12 = v3->inputedPinLen;
    v3->pinEntryInfo.mState = 0;
    v3->pinEntryInfo.mPinNumInputed = v12;
    *((_BYTE *)&pin_catcher_data + v12 + 984) = 0;
    v3->pinEntryInfo.mKeyCode = '*';
    if ( v3->pinEntryCfg.mPinLenTypes != 1 || v3->pinEntryCfg.mPinLenTypesList[0] != v12 )
      goto LABEL_11;
```

远程获取银行卡磁道信息

- 重打包com.lkl.cloudpos.payment
  - 禁用闪付
  - 禁用磁条卡类型校验
  - 打印卡口令
- 服务器收到卡磁道信息和口令
  - 复制卡盗刷