

Figure - Bug #114552

测试 Test-ST # 113421 (New): V4.0功能与专项测试
测试 Test-ST # 113425 (New): V4.0专项--BSP专项--压测

【BSP】【EVT1】【Boot】【偶现4/10】【压测】设备烧机后，在启动过程中断电重启，设备进入900E
2022-12-14 13:42 - 移动测试一组_CDTs 刘强

Status:	CLOSED	Start date:	2022-12-14
Priority:	High	Due date:	2023-01-19
Assignee:	移动测试一组_CDTs 刘强	% Done:	100%
Category:	BSP	Estimated time:	0.00 hour
Target version:	VC1_FSE_0086_20230328	Found Version:	FlatBuild_HH_VX1_MCE_FSE.M.D.user.01.00.X101.2
Need_Info:	--	Degrated:	Yes
Resolution:	FIXED	Verified Version:	
Severity:	Major	Fixed Version:	
Reproducibility:	Frequently	Root cause:	第一次开机过程中断电，导致文件系统损坏重启失
Test Type:	ST		

Description
【前提条件】 None
【测试步骤】 1.使用Qfile烧机后等待设备自动开机 2.在出现开机动画5s-10s左右断开电源然后重新插入 3.然后等待设备再次启动 4.再烧机重复1-3 10次
【预期结果】 3-4 均能正常启动
【实际结果】 设备启动失败进入900e

History
#1 - 2022-12-14 15:01 - CD SYSTEM-胡兵
- Status changed from New to ASSIGNED
- Assignee changed from CD SYSTEM-胡兵 to CD BSP-杜磊

Hi 杜磊
串口分析900E原因为，内核操作了非法的虚拟地址，调用栈如下
Pre_figure_turbox-c2130c-la1.1-vendor-dev/LINUX/android/kernel/msm-4.19/techpack/display/msm/sde/sde_kms.c
Pre_figure_turbox-c2130c-la1.1-vendor-dev/LINUX/android/kernel/msm-4.19/techpack/display/msm/msm_smmu.c
Pre_figure_turbox-c2130c-la1.1-vendor-dev/LINUX/android/kernel/msm-4.19/techpack/display/msm/msm_gem_vma.c
_sde_kms_mmu_init-- [drm: sde kms mmu init:3197]failed to map ret:-19
-- _sde_kms_map_all_splash_regions
---- _sde_kms_splash_mem_get-- [drm: sde kms splash_mem_get:794]splash memory smmu map failed:-19
----- mmu->funcs->one_to_one_map
----- msm_smmu_one_to_one_map

```

161         if (!client || !client->domain)
162             return -ENODEV;
    返回ENODEV，可能是前面没有初始化成功

--3219     fail:
--3221         _sde_kms_mmu_destroy(sde_kms);
----- msm_gem_address_space_put(sde_kms->aspace[i]);
----- msm_gem_address_space_destroy
----- aspace->ops->destroy(aspace)
----- smmu_aspace_destroy
----- aspace->mmu->funcs->destroy(aspace->mmu); -- Unable to handle kernel paging request at virtual address 51946e15c56007b7
----- static void msm_smmu_destroy(struct msm_mmu *mmu)
----- 210         kfree(smmu);

```

drm初始化过程中，检测到client/domain不存在，导致初始化失败，走fail流程，在destroy对应地址时出现非法访问。

需要详细check此部分加载时序是否正常，对比正常日志，目前还有一个怀疑点可供参考：

出现异常的开机日志中，没有msmdrm_smmu 相关打印，kfree的对象恰好又是smmu

```

行 275: [ 0.000000] Booting Linux on physical CPU 0x0000000000 [0x51df805e]
行 1568: [ 12.084444] msmdrm_smmu ae00000.qcom,mdss_mdp.qcom,smmu_sde_unsec_cb: Linked as a consumer to 150000000.apps-smmu
行 1572: [ 12.113792] msmdrm_smmu ae00000.qcom,mdss_mdp.qcom,smmu_sde_sec_cb: Linked as a consumer to 150000000.apps-smmu
行 1891: [ 0.000000] Booting Linux on physical CPU 0x0000000000 [0x51df805e]
行 4673: [ 31.656867] msmdrm_smmu ae00000.qcom,mdss_mdp.qcom,smmu_sde_unsec_cb: Linked as a consumer to 150000000.apps-smmu
行 4680: [ 31.714054] msmdrm_smmu ae00000.qcom,mdss_mdp.qcom,smmu_sde_sec_cb: Linked as a consumer to 150000000.apps-smmu
行 5324: [ 0.000000] Booting Linux on physical CPU 0x0000000000 [0x51df805e]
行 7469: [ 21.876227] [drm:_sde_kms_mmu_init:3197] [sde error]failed to map ret:-19
行 7487: [ 21.876286] pc : smmu_aspace_destroy+0x14/0x28

```

Thanks.

#2 - 2022-12-14 18:29 - CDTs-TEST 周婷

- Target version set to VX1_MCE_FSE_V5.0_20221230

#3 - 2022-12-14 18:31 - CDTs-TEST 周婷

- Due date set to 2022-12-17

此bug 需在12/20 工厂版本上进行修改

#4 - 2022-12-14 18:35 - CDTs-TEST 周婷

12/16 需有结论

#5 - 2022-12-23 12:47 - CD BSP-杜磊

- % Done changed from 0 to 10

1. log中出现000000000000地址，通常为0，出错后会kfree一个为0地址，导致panic

```

sde_kms_hw_init
rc = _sde_kms_hw_init_ioremap(sde_kms, platformdev);

```

```
sde_kms->mmio = msm_ioremap(platformdev, "mdp_phys", "mdp_phys");
if (IS_ERR(sde_kms->mmio)) {
rc = PTR_ERR(sde_kms->mmio);
SDE_ERROR("mdp register memory map failed: %d\n", rc);
sde_kms->mmio = NULL;
goto error;
}
DRM_INFO("mapped mdp address space @%pK\n", sde_kms->mmio); -->[ 21.875193] [drm] mapped mdp address space @0000000000000000
```

_sde_kms_hw_destroy(sde_kms, platformdev);

2. 51946e15c56007b7此地址为kernel请求的虚拟地址，此地址在内核和用户空间的虚拟地址，请求失败导致
Unable to handle kernel paging request at virtual address 51946e15c56007b7
[51946e15c56007b7] address between user and kernel address ranges

可以尝试规避panic的问题，但是会导致屏幕始终无法显示的问题

#6 - 2022-12-23 13:05 - CD BSP-杜磊

- Assignee changed from CD BSP-杜磊 to 移动测试一组_CDTS 刘强

hi，刘强，

帮忙用另外一台设备再复现一下此问题，并抓log

确认信息：

1. 新的设备复现此问题时，是否会出现同样的错误log, 若是，那说明此问题发生时，是同一个原因导致的。
若不是，那说明每台设备在启动时断电的随机性导致，此刻模块启动时发生异常。

从当前log分析看是display在初始化时出错导致系统进900E.

#7 - 2022-12-26 14:19 - CD BSP-杜磊

高通case: 06420013

#8 - 2022-12-27 18:52 - CD BSP-杜磊

- Status changed from ASSIGNED to NEED_INFO

#9 - 2022-12-28 20:03 - 移动测试一组_CDTS 刘强

- File teraterm.log added

- Assignee changed from 移动测试一组_CDTS 刘强 to CD BSP-杜磊

复现版本：FlatBuild_HH_VX1_MCE_FSE.M.R.user.01.00.0063.X101

出现错误日志：

```
[ 20.156381] Unable to handle kernel paging request at virtual address 007db129857b81e9
[ 20.155349] [drm] mapped mdp address space @0000000000000000
```

使用VX板子，之前是VC板子复现

#10 - 2023-01-04 10:48 - CDTs-TEST 周婷
- Status changed from NEED_INFO to ASSIGNED

#11 - 2023-01-05 10:18 - CD BSP-杜磊

当前关闭userdata加密，测试验证中

#12 - 2023-01-12 15:59 - CD TPM-王祥林
- Due date changed from 2022-12-17 to 2023-01-19

#13 - 2023-01-17 14:26 - CD BSP-杜磊
- Status changed from ASSIGNED to RESOLVED
- % Done changed from 10 to 90

问题修复，持续验证中，修改状态为RESOLVED，继续测试

#14 - 2023-01-18 17:03 - CD BSP-杜磊
- % Done changed from 90 to 100
- Degrated changed from -- to Yes

#15 - 2023-01-18 17:08 - CD BSP-杜磊
- Assignee changed from CD BSP-杜磊 to CD FW-王伟
- Resolution changed from -- to FIXED
- Root cause set to 第一次开机过程中断电，导致文件系统损坏重启失败进入900e

#16 - 2023-01-18 17:08 - CD BSP-杜磊
- Assignee changed from CD FW-王伟 to CDTs_TEST 王成

#17 - 2023-01-29 10:16 - CDTs_TEST 王成
- Assignee changed from CDTs_TEST 王成 to 移动测试一组_CDTs 刘强

麻烦跟进下工厂的生产情况，另外需要找周飞和唐金泽确认下一步解决方案，是否需要在开机动画出来前就完成数据备份

#18 - 2023-03-07 11:20 - 移动测试一组_CDTs 刘强

使用新的VB工厂版本和user来回压测验证：目前217次未复现

#19 - 2023-03-22 13:42 - 移动测试一组_CDTs 刘强

VB 验证 超过200次未复现，已经合入正式版本，继续在3.22 db 正式版本中压测，如不复现将关闭此问题

#20 - 2023-03-23 14:32 - CDTs_TEST 王成
- Target version changed from VX1_MCE_FSE_V5.0_20221230 to VC1_FSE_0086_20230328

#21 - 2023-03-27 14:25 - 移动测试一组_CDTs 刘强
- Status changed from RESOLVED to VERIFIED

VB验证200次
Release 0085版本验证：229次

- 【测试步骤】
1. 烧写0085版本
 2. 在开机过程中进行异常断电-上电压测 10次
 3. 等10次后，进入到操作系统，进行OTA升级
 4. 升级成功后，设备重启，在重启过程中进行异常断电压测

验证结果详情：<https://thundersoft.feishu.cn/sheets/shtcn7PGzO2W4gnMyIrmGfHFajh?sheet=FKdpGr>

#22 - 2023-03-27 14:25 - 移动测试一组_CDTS 刘强
- Status changed from VERIFIED to CLOSED

未复现key问题

Files			
1.txt	3.02 MB	2022-12-14	移动测试一组_CDTS 刘强
teraterm1.log	701 KB	2022-12-14	移动测试一组_CDTS 刘强
teraterm.log	4.12 MB	2022-12-28	移动测试一组_CDTS 刘强