Replicant - Issue #2104

Port the Replicant 6.0 fix for the Galaxy S III eMMC corruption bug in Replicant >= 9 kenrel

08/05/2020 04:46 PM - Denis 'GNUtoo' Carikli

Status:	Resolved	**Start date:**	08/05/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Replicant 11.0 0001	**Spent time:**	0.00 hour
Resolution:	fixed	**Grant:**	
Device:	Galaxy S 3 (I9300), Galaxy S 3 4G (I9305)	**Type of work:**	C programming

Description

History

#1 - 08/05/2020 04:47 PM - Denis 'GNUtoo' Carikli

- Subject changed from Investigate if the eMMC bug is fixed in Linux to Investigate if the Galaxy SIII eMMC corruption bug is also fixed in Linux upstream or just in SMDK4412

- Do we need to add quirks upstream, or is it already done?
- What does the smdk4412 kernel does to avoid triggering that bug?

#2 - 08/06/2020 01:34 PM - dl lud

The commit that fixes the eMMC failure in the smdk4412 kernel is this one: da8461692362317a8ffce4d4646953985fcf4e1d

The eMMC sudden death research thread at xda tries to explain this patch.

#3 - 08/06/2020 02:12 PM - dl lud

- Subject changed from Investigate if the Galaxy SIII eMMC corruption bug is also fixed in Linux upstream or just in SMDK4412 to Investigate if the Galaxy S III eMMC corruption bug is fixed in upstream Linux

- Device Galaxy S 3 (I9300) added

- Device deleted (Unknown)

Also note that the proper fix for the bug comes in a firmware update for the eMMC chip. Devices running the 0xF7 version of the VTU00M firmware should be ok and won't need a patched kernel.

#4 - 08/16/2020 10:42 PM - Denis 'GNUtoo' Carikli

Thanks. It describes things that the eMMC hacking, or: how I fixed long-dead Galaxy S3 phones talk doesn't like the smart report.

#5 - 08/23/2020 06:52 PM - Denis 'GNUtoo' Carikli

There is a link of eMMC fimrware bugs from the former CyanogenMod wiki here: https://undocumented.software/wiki_dump/EMMC_Bugs.html

#6 - 08/24/2020 10:04 PM - Denis 'GNUtoo' Carikli

- Target version changed from replicant 10.0 to Replicant 11.0 0001

#7 - 08/24/2020 10:16 PM - Denis 'GNUtoo' Carikli

- Subject changed from Investigate if the Galaxy S III eMMC corruption bug is fixed in upstream Linux to Investigate if the Galaxy S III eMMC corruption bug is fixed in upstream Linux and if not port the Replicant 6.0 fix

#8 - 08/24/2020 10:16 PM - Denis 'GNUtoo' Carikli

- Device Galaxy S 3 4G (I9305) added

#9 - 11/04/2020 01:21 AM - Denis 'GNUtoo' Carikli

- Subject changed from Investigate if the Galaxy S III eMMC corruption bug is fixed in upstream Linux and if not port the Replicant 6.0 fix to Port the Replicant 6.0 fix for the Galaxy S III eMMC corruption bug in Replicant >= 9 kenrel

#10 - 11/04/2020 01:24 AM - Denis 'GNUtoo' Carikli

The bug is not fixed upstream, so we at least need to port it in our kernels not to brick any devices.

On the GT-I9300, the bugfix isn't great as it's just patch to hang the eMMC when it's about to create corruption, but not having that patch would be way worse.

We also might want to warn users if they have affected eMMC firmwares or not.

#11 - 03/26/2021 06:53 PM - _I3^ RELATIVISM

- Type of work C programming added

#12 - 07/06/2021 04:46 PM - Denis 'GNUtoo' Carikli

- Belgin has ported the patch on top of Replicant 11 kernel , but we still need to test it and/or ask belgin if it's fine to import as-is and add ask permission to belgin to add a signed-off by by belgin before importing it.

I've done a bit more research on the bug to see how to upstream that patch:

- In mmc_start_movi_smart, it seems to enter enters some "Smart Report mode[1]" to check a date.
- There are MMC quirks too but the defines are in include/linux. We might be able to call it MMC_QUIRK_VT00M_0xF1_20120413_BUG or something like that as the bug causes some corruption in the FTL metadata which then crashes the eMMC CPU at the next boot. This patch just patches the eMMC firmware in RAM to make the eMMC CPU hang (by looping infinitely) when the corruption is about to happen. So we also need to do it before Linux gives access to the eMMC to userspace.
- In the presentation about resurecting i9300, the presenter said that he didn't investigate the cause of the bug enough to be able to produce a patched firmware where it is really fixed (instead of being workarounded with that Samsung patch). So without more information we probably need to stick to just patching the eMMC RAM in the same way but integrating it better with the quirk system that is already in place in Linux to enable upstream to accept it.

[1] https://android.googlesource.com/kernel/omap.git/+/7ec52272f810bd941af58ec87554e201d146934b/drivers/mmc/core/quirks.c

#13 - 07/08/2021 08:48 AM - Denis 'GNUtoo' Carikli

- Status changed from New to Resolved

- Resolution set to fixed

Since Belgin ported the patch, and that I now pushed it, we can consider it as fixed.

Another bug (#2267) has been opened for upstreaming that patch.

Thanks a lot for the patch.

I'll also update the wiki to not warn about it anymore, or at least not in the same way.