Replicant - Issue #735

emmc secure erase bug

12/12/2013 07:20 PM - Andrew Engelbrecht

Status:	Closed	**Start date:**	12/12/2013
Priority:	Urgent	**Due date:**	
Assignee:	Paul Kocialkowski	**% Done:**	0%
Category:	Framework	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:	fixed	**Grant:**	
Device:	Galaxy S 2 (I9100)	**Type of work:**	

Description

ok, the following issue does apply to replicant:

http://wiki.cyanogenmod.org/w/EMMC_Bugs#Samsung_eMMC_secure_erase_bug

the mentioned kernel patch has not been applied in replicant. (compare:)

https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3550ccd
https://gitorious.org/replicant/kernel_samsung_smdk4210/source/e246554a76666c3b1e521f15e224b86f5917daed:drivers/mmc/card/block.c

if you'd like, i could create a brief warning on the install page, like the one at the top, here: http://wiki.cyanogenmod.org/w/I9100_Info <- this is my offer to help.

my phone's flash chip is an affected model. i'm nearly positive that my flash chip is partly corrupted. (reading sequential 1 MB blocks from my flash chip with dd gives about 6.8 thousand errors. somehow, the affected areas doesn't prevent my phone from booting, or show obvious data corruption during day-to-day use. it's an absolute paradox, but the issue remains that the kernels shipped with replicant are **not** patched to work around this dangerous firmware bug.)

this bug also affects some galaxy s3 phones. there is a work-around available for them too. see:
http://wiki.cyanogenmod.org/w/EMMC_Bugs

sorry for taking a while to open a new bug report about this.

History

#1 - 12/15/2013 07:47 PM - Paul Kocialkowski

Can you check whether the cm-10.1 branches of the CM kernels include those fixes (or equivalent ones). If so, please tell me exactly what patch to backport. I am not sure the one from mainline will work on the Samsung Android tree.

#2 - 12/15/2013 08:12 PM - Andrew Engelbrecht

github search is broken, and has been for a while. (searching for CM repos containing the word "bash" or "4210" bring up nothing, even though there are repos named that.) Do you know the url for the repo you forked from? i'll keep looking for it.

last time i was looking at the kernel tree for the i9100, i noticed that there were no 9.0 branches or tags anymore. i'll look for the relevant patch in 10.1.

#3 - 12/15/2013 08:15 PM - Andrew Engelbrecht

found what i was looking for. i believe it's this one:

https://github.com/CyanogenMod/android_kernel_samsung_smdk4210

#4 - 12/15/2013 08:39 PM - Andrew Engelbrecht

sorry about all that uncertainty. i found the patch for the relevant file:

https://github.com/CyanogenMod/android_kernel_samsung_smdk4210/blob/17c7b6e39ed37cb9fed9bb0b66c152ea4be299c4/drivers/mmc/card/block.c

it's a pretty *huge* patch, changing lots of files. it looks like they may have taken a flat diff from some other git repo.

i was wondering if it would hurt to use the newer kernel versions modified by cyanogenmod. however, it could be a lot of work for the linux-libre folk. i guess you could cherry pick the changes to that file, and compare to the patch in mainline?

thanks for addressing this! :)

#5 - 12/16/2013 01:42 PM - Paul Kocialkowski

Galaxy S2's repo is: https://github.com/CyanogenMod/android_kernel_samsung_smdk4210
Galaxy S3's repo is: https://github.com/CyanogenMod/android_kernel_samsung_smdk4412
Now starting with CM 10.1, only the SMDK4412 kernel is used for both devices.

> it's a pretty huge patch, changing lots of files. it looks like they may have taken a flat diff from some other git repo.

Yes, they actually import the kernel source code as released by Samsung which doesn't contain any git infos.

Are you sure this contains a fix?

> i was wondering if it would hurt to use the newer kernel versions modified by cyanogenmod.

We're going to use the cm-10.2 branch kernels starting with the Replicant 4.2 release, so if they do contain the fix, we could use it. Now can you tell which kernel and branch from CM has or doesn't have the patch? Maybe they need to patch these issues first so that we can inherit the patches (would make more sense than only patching Replicant).

> however, it could be a lot of work for the linux-libre folk. i guess you could cherry pick the changes to that file, and compare to the patch in mainline?

We **do not** use Linux-libre. Our kernel is directly the CyanogenMod kernel from which we removed the firmwares, so we do inherit any of their improvements. I am a bit under the impression that you thought we were using mainline Linux or Linux-libre!

#6 - 12/18/2013 02:33 AM - Andrew Engelbrecht

after a quick visual check, it appears branches with this commit may be patched:

https://github.com/CyanogenMod/android_kernel_samsung_smdk4412
```
    2489007e7d740ccbc3e0a202914e243ad5178787
```

i did a visual inspection with the mainline patch, as automatic reverse patching fails:

https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3550ccd

the cm-10.1, cm-10.2 and cm-11.0 branches may have that commit. i didn't download the git tree myself, but doing so may make verification easier.

regarding the linux-libre folk, i was referring to anyone who spends time de-blobbing the kernel you use. i was concerned that checking for blob changes might be hard. anyhow, i'm a fan of incremental improvements regarding sw freedom, instead of up front perfection. :-)

#7 - 12/20/2013 01:17 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Okay so I suppose this means the Replicant 4.2 release will include the fix. I doubt we'll ever do new images of 4.0 for the affected devices, so let's say the issue is closed.

#8 - 01/17/2015 03:19 PM - Paul Kocialkowski

- Target version changed from 21 to Any version

#9 - 12/15/2015 01:06 PM - Denis 'GNUtoo' Carikli

- Category changed from 81 to Framework

- Device Galaxy S 2 (I9100) added