

Re: [PATCH 3/7] inflate pt1: clean up input logic

Re: [PATCH 3/7] inflate pt1: clean up input logic

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-02/msg09562.html>

- *From:* Russell King <rmk+lkml@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 27 Feb 2006 15:47:49 +0000
-

On Mon, Feb 27, 2006 at 01:07:29PM +0100, Johannes Stezenbach wrote:

On Mon, Feb 27, 2006, Russell King wrote:

On Mon, Feb 27, 2006 at 02:18:44AM +0100, Johannes Stezenbach wrote:

On Sat, Feb 25, 2006 at 10:57:49PM +0000, Russell King wrote:

The email:

<http://www.ussg.iu.edu/hypermail/linux/kernel/0312.2/1024.html>

contains a full and clear explanation of the situation. The second paragraph of that email is key to understanding the problem and makes it absolutely clear what is trying to be decompressed as the initrd (the corrupted compressed piggy).

FWIW, I didn't it either. "Work around broken boot firmware which passes invalid initrd to kernel" would have been a simpler description.

Sigh, I'm sick of this crap. I'm not going to debate it any further.

I agree that it would be nice if inflate.c would fail gracefully instead of halting,

IT _DOES_ FAIL GRACEFULLY TODAY. WITH MATT'S PATCHES, IT
DOESN'T.
THAT'S A REGRESSION. WHAT IS IT ABOUT THAT WHICH PEOPLE
DON'T

Re: [PATCH 3/7] inflate pt1: clean up input logic

UNDERSTAND? DO I HAVE TO SPELL IT OUT IN ONE SYLLABLE WORDS?

I got that already, no need to shout. I just wanted to point out that from the information you provided so far it looks like your problem could be fixed in a more straight forward fashion.

Problem: Boot firmware passes invalid arguments.
Solution: Ignore invalid boot firmware arguments.

Let me try to explain – but I doubt it'll do any good because folk don't seem to understand plain English here anymore (or at least that's what it seems like from `_my_` perspective.)

In order to detect that the arguments are invalid, you'd need to validate the `initrd`.

In order to validate a compressed `initrd`, you'd have to `uninflate` it, just like `gunzip -t`.

(a) `gunzip -t` is able to work because it has `setjmp/longjmp`, so when it runs out of data, it can sanely exit from the data reading function when it encounters insufficient data.

The kernel does not have such functionality, and it has been determined long ago that the kernel shall not have such functionality – it was discussed at the time when this problem first came up and the resounding answer was precisely as I state.

(b) if we have to have separate code to validate a compressed image, that is a complete waste of code and resources – we already have something which tests whether a compressed image is valid by inflating it – called `lib/inflate.c`.

So, your suggestion isn't a really a solution when the simple solution is to keep the original `_simple_` fix for a buggy integration of the `gzip` inflate code.

but why can't you just use
`CONFIG_BLK_DEV_INITRD=n`?

Because you might want to use an `initrd` for real (for installation purposes) and therefore distributions (eg Debian) want it turned on?

If you use a distribution kernel which contains one, you

Re: [PATCH 3/7] inflate pt1: clean up input logic

Re: [PATCH 3/7] inflate pt1: clean up input logic

could simply add "noinitrd" to the kernel command line
to ignore it, no?

Tell that to all the people who have complained in the past about it.

Okay, this does it – I'm ignoring further discussion on this stupid
idiotic topic which is soo bloody difficult for others to understand.

I don't understand your aggressiveness, there must be a dark
secret behind all this. Or maybe it's just the season
for flame wars.

I'm completely and utterly pissed off with this thread, having to almost
go back to kindergarten type explanations to get the point across.
That's what has been soo infuriating about this whole saga.

And what's even more stupid is the attitude that required fixes can be
thrown out of the kernel, and then a massive argument is required to
re-explain wtf they're necessary.

Are we doomed to have to repeatedly explain why bug fixes are necessary?
If that's the case, let's pack up this Linux kernel thing because we're
on a route to insanity.

--

Russell King
Linux kernel 2.6 ARM Linux – <http://www.arm.linux.org.uk/>
maintainer of: 2.6 Serial core

–

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in
the body of a message to majordomo@xxxxxxxxxxxxxxxxx
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>