[PATCH v2] fs/squashfs: Use kcalloc when relevant

Miquel Raynal miquel.raynal at bootlin.com
Mon Jun 27 12:20:03 CEST 2022

- Previous message (by thread): [GIT PULL] xilinx patches for v2022.10
- Next message (by thread): [PATCH v2] fs/squashfs: Use kcalloc when relevant
- **Messages sorted by:** [date] [thread] [subject] [author]

```
A crafted squashfs image could embed a huge number of empty metadata
blocks in order to make the amount of malloc()'d memory overflow and be
much smaller than expected. Because of this flaw, any random code
positioned at the right location in the squashfs image could be memcpy'd
from the squashfs structures into U-Boot code location while trying to
access the rearmost blocks, before being executed.

In order to prevent this vulnerability from being exploited in eg. a
secure boot environment, let's add a check over the amount of data
that is going to be allocated. Such a check could look like:

if (!elem_size || n > SIZE_MAX / elem_size)
        return NULL;

The right way to do it would be to enhance the calloc() implementation
but this is quite an impacting change for such a small fix. Another
solution would be to add the check before the malloc call in the
squashfs implementation, but this does not look right. So for now, let's
use the kcalloc() compatibility function from Linux, which has this
check.

Fixes: c5100613037 ("fs/squashfs: new filesystem")
Reported-by: Tatsuhiko Yasumatsu <Tatsuhiko.Yasumatsu at sony.com>
Signed-off-by: Miquel Raynal <miquel.raynal at bootlin.com>
Tested-by: Tatsuhiko Yasumatsu <Tatsuhiko.Yasumatsu at sony.com>
---

Changes in v2:
* Fixed the title prefix: s/sqashfs/squashfs
* Rebased on master to avoid a conflit with a headers change
* Added a Fixes tag
* Added the Tested-by from Tatsuhiko sent privately

 fs/squashfs/sqfs.c | 4 +++-
 1 file changed, 3 insertions(+), 1 deletion(-)

diff --git a/fs/squashfs/sqfs.c b/fs/squashfs/sqfs.c
index 40361ffa6d6..9f98d086070 100644
--- a/fs/squashfs/sqfs.c
+++ b/fs/squashfs/sqfs.c
@@ -13,6 +13,7 @@
 #include <fs.h>
 #include <linux/types.h>
 #include <asm/byteorder.h>
+#include <linux/compat.h>
 #include <memalign.h>
 #include <stdlib.h>
 #include <string.h>
@@ -726,7 +727,8 @@ static int sqfs_read_inode_table(unsigned char **inode_table)
                 goto free_itb;
         }
```

```
-       *inode_table = malloc(metablks_count * SQFS_METADATA_BLOCK_SIZE);
+       *inode_table = kcalloc(metablks_count, SQFS_METADATA_BLOCK_SIZE,
+                              GFP_KERNEL);
        if (!*inode_table) {
                ret = -ENOMEM;
                printf("Error: failed to allocate squashfs inode_table of size %i, increasing
CONFIG_SYS_MALLOC_LEN could help\n",
--
2.34.1
```

- Previous message (by thread): [GIT PULL] xilinx patches for v2022.10
- Next message (by thread): [PATCH v2] fs/squashfs: Use kcalloc when relevant
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the U-Boot mailing list