From: Miquel Raynal <miquel.raynal@bootlin.com>
To: u-boot@lists.denx.de
Cc: Thomas Petazzoni <thomas.petazzoni@bootlin.com>,
Joao Marcos Costa <joaomarcos.costa@bootlin.com>,
Miquel Raynal <miquel.raynal@bootlin.com>,
Jincheng Wang <jc.w4ng@gmail.com>
Subject: [PATCH v2] fs/squashfs: sqfs_read: Prevent arbitrary code execution
Date: Thu, 9 Jun 2022 16:02:06 +0200 [thread overview]
Message-ID: <20220609140206.297405-1-miquel.raynal@bootlin.com> (raw)

Following Jincheng's report, an out-of-band write leading to arbitrary
code execution is possible because on one side the squashfs logic
accepts directory names up to 65535 bytes (u16), while U-Boot fs logic
accepts directory names up to 255 bytes long.

Prevent such an exploit from happening by capping directory name sizes
to 255. Use a define for this purpose so that developers can link the
limitation to its source and eventually kill it some day by dynamically
allocating this array (if ever desired).

Link: https://lore.kernel.org/all/CALO=DHFB+yBoXxVr5KcsK0iFdg+e7ywko4-e+72kjbcS8JBfPw@mail.gmail.com
Reported-by: Jincheng Wang <jc.w4ng@gmail.com>
Signed-off-by: Miquel Raynal <miquel.raynal@bootlin.com>

Changes in v2:
* Jincheng reported in private that there was a problem with small name
  sizes, the last byte was lost. The reason is, dirs->entry->name_size
  contains the length of the string minus one (and excluding the
  trailing '\0'). The previous implementation had this handled correctly
  but my initial fix did not kept the "+ 1" in place because it felt
  wrong but is actually necessary. This information is actually
  available in a comment a bit above in this file.

 fs/squashfs/sqfs.c | 8 +++++---
 include/fs.h | 4 +++-
 2 files changed, 8 insertions(+), 4 deletions(-)

```
diff --git a/fs/squashfs/sqfs.c b/fs/squashfs/sqfs.c
index b4484fa17f5..3f1030057c4 100644
--- a/fs/squashfs/sqfs.c
+++ b/fs/squashfs/sqfs.c
@@ -976,6 +976,7 @@ int sqfs_readdir(struct fs_dir_stream *fs_dirs, struct fs_dirent **dentp)
        int i_number, offset = 0, ret;
        struct fs_dirent *dent;
        unsigned char *ipos;
+       u16 name_size;

        dirs = (struct squashfs_dir_stream *)fs_dirs;
        if (!dirs->size) {
@@ -1058,9 +1059,10 @@ int sqfs_readdir(struct fs_dir_stream *fs_dirs, struct fs_dirent
**dentp)
                return -SQFS_STOP_READDIR;
        }

-       /* Set entry name */
-       strncpy(dent->name, dirs->entry->name, dirs->entry->name_size + 1);
-       dent->name[dirs->entry->name_size + 1] = '\0';
+       /* Set entry name (capped at FS_DIRENT_NAME_LEN which is a U-Boot limitation) */
```

```
+       name_size = min_t(u16, dirs->entry->name_size + 1, FS_DIRENT_NAME_LEN - 1);
+       strncpy(dent->name, dirs->entry->name, name_size);
+       dent->name[name_size] = '\0';

        offset = dirs->entry->name_size + 1 + SQFS_ENTRY_BASE_LENGTH;
        dirs->entry_count--;
diff --git a/include/fs.h b/include/fs.h
index b43f16a692f..2195dc172ec 100644
--- a/include/fs.h
+++ b/include/fs.h
@@ -174,6 +174,8 @@ int fs_write(const char *filename, ulong addr, loff_t offset, loff_t len,
 #define FS_DT_REG  8         /* regular file */
 #define FS_DT_LNK  10        /* symbolic link */

+#define FS_DIRENT_NAME_LEN 256
+
 /**
  * struct fs_dirent - directory entry
  *
@@ -194,7 +196,7 @@ struct fs_dirent {
        /** change_time:        time of last modification */
        struct rtc_time change_time;
        /** name:               file name */
-       char name[256];
+       char name[FS_DIRENT_NAME_LEN];
 };

 /* Note: fs_dir_stream should be treated as opaque to the user of fs layer */
--
2.34.1
```

Reply instructions:

You may reply publicly to this message via plain-text email
using any one of the following methods:

* Save the following mbox file, import it into your mail client,
  and reply-to-all from there: mbox

  Avoid top-posting and favor interleaved quoting:
  https://en.wikipedia.org/wiki/Posting_style#Interleaved_style

* Reply using the **--to**, **--cc**, and **--in-reply-to**
  switches of git-send-email(1):

  git send-email \
    --in-reply-to=20220609140206.297405-1-miquel.raynal@bootlin.com \
    --to=miquel.raynal@bootlin.com \
    --cc=jc.w4ng@gmail.com \

```
    --cc=joaomarcos.costa@bootlin.com \
    --cc=thomas.petazzoni@bootlin.com \
    --cc=u-boot@lists.denx.de \
    /path/to/YOUR_REPLY
```

  https://kernel.org/pub/software/scm/git/docs/git-send-email.html

* If your mail client supports setting the **In-Reply-To** header
  via mailto: links, try the mailto: link

Be sure your reply has a **Subject:** header at the top and a blank line before the message body.
