

[U-Boot] [PATCH 5/5] CVE-2019-13106: ext4: fix out-of-bounds memset

Paul Emge [paulemge at forallsecure.com](mailto:paulemge@forallsecure.com)

Mon Jul 8 23:37:07 UTC 2019

- Previous message: [\[U-Boot\].\[PATCH 4/5\] ext4: gracefully fail on divide-by-0](#)
- Next message: [\[U-Boot\].\[PATCH 5/5\] CVE-2019-13106: ext4: fix out-of-bounds memset](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

In ext4fs_read_file in ext4fs.c, a memset can overwrite the bounds of the destination memory region. This patch adds a check to disallow this.

Signed-off-by: Paul Emge <[paulemge at forallsecure.com](mailto:paulemge@forallsecure.com)>

```

---
 fs/ext4/ext4fs.c | 7 +++++--
 1 file changed, 5 insertions(+), 2 deletions(-)

diff --git a/fs/ext4/ext4fs.c b/fs/ext4/ext4fs.c
index e2b740cac4..37b31d9f0f 100644
--- a/fs/ext4/ext4fs.c
+++ b/fs/ext4/ext4fs.c
@@ -61,6 +61,7 @@ int ext4fs_read_file(struct ext2fs_node *node, loff_t pos,
     lbaint_t delayed_skipfirst = 0;
     lbaint_t delayed_next = 0;
     char *delayed_buf = NULL;
+    char *start_buf = buf;
     short status;
     struct ext_block_cache cache;

@@ -139,6 +140,7 @@ int ext4fs_read_file(struct ext2fs_node *node, loff_t pos,
     }
     } else {
+        int n;
+        int n_left;
         if (previous_block_number != -1) {
             /* spill */
             status = ext4fs_devread(delayed_start,
@@ -153,8 +155,9 @@ int ext4fs_read_file(struct ext2fs_node *node, loff_t pos,
         }
         /* Zero no more than `len' bytes. */
         n = blocksize - skipfirst;
-        if (n > len)
+        n = len;
+        n_left = len - ( buf - start_buf );
+        if (n > n_left)
+            n = n_left;
         memset(buf, 0, n);
     }
     buf += blocksize - skipfirst;
--
2.20.1

```

- Previous message: [\[U-Boot\].\[PATCH 4/5\] ext4: gracefully fail on divide-by-0](#)
- Next message: [\[U-Boot\].\[PATCH 5/5\] CVE-2019-13106: ext4: fix out-of-bounds memset](#)

- **Messages sorted by:** [[date](#)] [[thread](#)] [[subject](#)] [[author](#)]
-

[More information about the U-Boot mailing list](#)