Subject: [PATCH] EXT3: ext3 block bitmap leakage
Posted by Kirill Korotaev on Fri, 30 Jun 2006 09:41:05 GMT
View Forum Message <> Reply to Message

Andrew, Chris,

this bug is not relevant for 2.6.17 and later.
However, it is relevant for all 2.4.x and <2.6.17 kernels,
so I think this can be of interest to some people and worth commiting to
2.6.16.x

This patch fixes ext3 block bitmap leakage,
which leads to the following fsck messages on
healthy filesystem:
Block bitmap differences: -64159 -73707

All kernels up to 2.6.17 have this bug.

Found by
  Vasily Averin <vvs@sw.ru> and Andrey Savochkin <saw@sawoct.com>
Test case triggered the issue was created by
  Dmitry Monakhov <dmonakhov@sw.ru>

Signed-Off-By: Vasiliy Averin <vvs@sw.ru>
Signed-Off-By: Andrey Savochkin <saw@sawoct.com>
Signed-Off-By: Kirill Korotaev <dev@openvz.org>
CC: Dmitry Monakhov <dmonakhov@sw.ru>

```
--- ./fs/ext3/inode.c.e3crp 2006-06-28 05:22:40.000000000 +0400
+++ ./fs/ext3/inode.c 2006-06-27 13:31:20.000000000 +0400
@@ -585,6 +585,7 @@ static int ext3_alloc_branch(handle_t *h

   branch[0].key = cpu_to_le32(parent);
   if (parent) {
+  keys = 1;
    for (n = 1; n < num; n++) {
     struct buffer_head *bh;
     /* Allocate the next block */
```