



author Edward Adam Davis <eadavis@qq.com> 2025-02-20 19:24:19 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2025-05-02 07:39:10 +0200
commit a065cec230aa807c18828a3eee82f1c8592c2adf (patch)
tree f7bc79b653ed3cb341097a51efdc64e07786701e
parent 5b2f26d3fba4e9aac314f8bc0963b3fc28c0e456 (diff)
download linux-a065cec230aa807c18828a3eee82f1c8592c2adf.tar.gz

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

jfs: add sanity check for agwidth in dbMount

[Upstream commit ddf2846f22e8575d6b4b6a66f2100f168b8cd73d]

The width in dmapctl of the AG is zero, it trigger a divide error when calculating the control page level in dbAllocAG.

To avoid this issue, add a check for agwidth in dbAllocAG.

Reported-and-tested-by: syzbot+7c808908291a569281a9@syzkaller.appspotmail.com

Closes: <https://syzkaller.appspot.com/bug?extid=7c808908291a569281a9>

Signed-off-by: Edward Adam Davis <eadavis@qq.com>

Signed-off-by: Dave Kleikamp <dave.kleikamp@oracle.com>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- fs/jfs/jfs_dmap.c 4
```

1 files changed, 4 insertions, 0 deletions

diff --git a/fs/jfs/jfs_dmap.c b/fs/jfs/jfs_dmap.c

index d4e26744b2005b..d161bbafe77f61 100644

--- a/fs/jfs/jfs_dmap.c

+++ b/fs/jfs/jfs_dmap.c

```
@@ -204,6 +204,10 @@ int dbMount(struct inode *ipbmap)
     bmp->db_aglevel = le32_to_cpu(dbmp_le->dn_aglevel);
     bmp->db_agheight = le32_to_cpu(dbmp_le->dn_agheight);
     bmp->db_agwidth = le32_to_cpu(dbmp_le->dn_agwidth);
+    if (!bmp->db_agwidth) {
+        err = -EINVAL;
+        goto err_release_metapage;
+    }
     bmp->db_agstart = le32_to_cpu(dbmp_le->dn_agstart);
     bmp->db_agl2size = le32_to_cpu(dbmp_le->dn_agl2size);
     if (bmp->db_agl2size > L2MAXL2SIZE - L2MAXAG ||
```