torvalds / **linux** Public

Code   Pull requests 312   Actions   Projects   Security   Insights

btrfs: fix NULL pointer dereference when deleting device by invalid id

Browse files

```
[BUG]
It's easy to trigger NULL pointer dereference, just by removing a
non-existing device id:

 # mkfs.btrfs -f -m single -d single /dev/test/scratch1 \
                                     /dev/test/scratch2
 # mount /dev/test/scratch1 /mnt/btrfs
 # btrfs device remove 3 /mnt/btrfs

Then we have the following kernel NULL pointer dereference:

 BUG: kernel NULL pointer dereference, address: 0000000000000000
 #PF: supervisor read access in kernel mode
 #PF: error_code(0x0000) - not-present page
 PGD 0 P4D 0
 Oops: 0000 [#1] PREEMPT SMP NOPTI
 CPU: 9 PID: 649 Comm: btrfs Not tainted 5.14.0-rc3-custom+ #35
 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015
 RIP: 0010:btrfs_rm_device+0x4de/0x6b0 [btrfs]
  btrfs_ioctl+0x18bb/0x3190 [btrfs]
  ? lock_is_held_type+0xa5/0x120
  ? find_held_lock.constprop.0+0x2b/0x80
  ? do_user_addr_fault+0x201/0x6a0
  ? lock_release+0xd2/0x2d0
  ? __x64_sys_ioctl+0x83/0xb0
  __x64_sys_ioctl+0x83/0xb0
  do_syscall_64+0x3b/0x90
  entry_SYSCALL_64_after_hwframe+0x44/0xae

[CAUSE]
Commit a27a94c ("btrfs: Make btrfs_find_device_by_devspec return
btrfs_device directly") moves the "missing" device path check into
btrfs_rm_device().

But btrfs_rm_device() itself can have case where it only receives
@devid, with NULL as @device_path.

In that case, calling strcmp() on NULL will trigger the NULL pointer
dereference.

Before that commit, we handle the "missing" case inside
btrfs_find_device_by_devspec(), which will not check @device_path at all
if @devid is provided, thus no way to trigger the bug.

[FIX]
Before calling strcmp(), also make sure @device_path is not NULL.

Fixes: a27a94c ("btrfs: Make btrfs_find_device_by_devspec return btrfs_device directly")
CC: stable@vger.kernel.org # 5.4+
Reported-by: butt3rflyh4ck <butterflyhuangxx@gmail.com>
Reviewed-by: Anand Jain <anand.jain@oracle.com>
Signed-off-by: Qu Wenruo <wqu@suse.com>
Reviewed-by: David Sterba <dsterba@suse.com>
Signed-off-by: David Sterba <dsterba@suse.com>
```

master

v6.1 … v5.15-rc1

adam900710 authored and **kdave** committed on Aug 23, 2021 1 parent 63fb587 commit e4571b8c5e9ffa1e85c0c671995bd4dcc5c75091

Showing **1 changed file** with **1 addition** and **1 deletion**.

Split Unified

2 fs/btrfs/volumes.c

```

         if (IS_ERR(device)) {
                 if (PTR_ERR(device) == -ENOENT &&
-                    strcmp(device_path, "missing") == 0)
+                    device_path && strcmp(device_path, "missing") == 0)
                         ret = BTRFS_ERROR_DEV_MISSING_NOT_FOUND;
                 else
                         ret = PTR_ERR(device);
```

0 comments on commit e4571b8

Please sign in to comment.