



author Xiubo Li <xiubli@redhat.com> 2022-11-09 11:00:39 +0800
committer Ilya Dryomov <idryomov@gmail.com> 2022-11-14 10:29:05 +0100
commit [51884d153f7ec85e18d607b2467820a90e0f4359](#) (patch)
tree [1f86a0506cd2e12498a2bc6cf3bec781d11c9342](#)
parent [f86a48667b91202d502d753c707e8576a6fe265b](#) (diff)
download [linux-51884d153f7ec85e18d607b2467820a90e0f4359.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

ceph: avoid putting the realm twice when decoding snaps fails

When decoding the snaps fails it maybe leaving the 'first_realm' and 'realm' pointing to the same snaprealm memory. And then it'll put it twice and could cause random use-after-free, BUG_ON, etc issues.

Cc: stable@vger.kernel.org

Link: <https://tracker.ceph.com/issues/57686>

Signed-off-by: Xiubo Li <xiubli@redhat.com>

Reviewed-by: Ilya Dryomov <idryomov@gmail.com>

Signed-off-by: Ilya Dryomov <idryomov@gmail.com>

Diffstat

```
-rw-r--r-- fs/ceph/snap.c 3
```

1 files changed, 2 insertions, 1 deletions

diff --git a/fs/ceph/snap.c b/fs/ceph/snap.c

index 864cdaa0d2bd65..e4151852184e04 100644

--- a/fs/ceph/snap.c

+++ b/fs/ceph/snap.c

```
@@ -763,7 +763,7 @@ int ceph_update_snap_trace(struct ceph_mds_client *mdsc,
    struct ceph_mds_snap_realm *ri; /* encoded */
    __le64 *snaps; /* encoded */
    __le64 *prior_parent_snaps; /* encoded */
-   struct ceph_snap_realm *realm = NULL;
+   struct ceph_snap_realm *realm;
    struct ceph_snap_realm *first_realm = NULL;
    struct ceph_snap_realm *realm_to_rebuild = NULL;
    int rebuild_snapcs;

@@ -774,6 +774,7 @@ int ceph_update_snap_trace(struct ceph_mds_client *mdsc,

    dout("%s deletion=%d\n", __func__, deletion);

more:
+   realm = NULL;
    rebuild_snapcs = 0;
    ceph_decode_need(&p, e, sizeof(*ri), bad);
    ri = p;
```