



author Dan Carpenter <error27@gmail.com> 2022-11-15 16:16:43 +0300
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:36:50 +0100
commit [fc1897f16ebcfd22364f2afcc27f53a740f3bc7a](#) (patch)
tree [37d797e44d6c9eec07e284b3be53d6a9ad4d2b7a](#)
parent [7ed540bcee2e24479524b9705cc7462b2652f944](#) (diff)
download [linux-fc1897f16ebcfd22364f2afcc27f53a740f3bc7a.tar.gz](#)

diff options

context:
space:
mode:

drbd: use after free in drbd_create_device()

[Upstream commit [a7a1598189228b5007369a9622ccdf587be0730f](#)]

The `drbd_destroy_connection()` frees the "connection" so use the `_safe()` iterator to prevent a use after free.

Fixes: [b6f85ef9538b](#) ("drbd: Iterate over all connections")

Signed-off-by: Dan Carpenter <error27@gmail.com>

Reviewed-by: Christoph Böhmwalder <christoph.boehmwalder@linbit.com>

Link: <https://lore.kernel.org/r/Y3Jd5iZRbNQ9w6gm@kili>

Signed-off-by: Jens Axboe <axboe@kernel.dk>

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

Diffstat

```
-rw-r--r-- drivers/block/drbd/drbd_main.c 4
```

1 files changed, 2 insertions, 2 deletions

diff --git a/drivers/block/drbd/drbd_main.c b/drivers/block/drbd/drbd_main.c

index 1e02cb60b65b6d..872e70f5b4d67e 100644

--- a/drivers/block/drbd/drbd_main.c

+++ b/drivers/block/drbd/drbd_main.c

@@ -2804,7 +2804,7 @@ static int init_submitter(struct drbd_device *device)

enum drbd_ret_code drbd_create_device(struct drbd_config_context *adm_ctx, unsigned int minor)
{

struct drbd_resource *resource = adm_ctx->resource;

- struct drbd_connection *connection;

+ struct drbd_connection *connection, *n;

struct drbd_device *device;

struct drbd_peer_device *peer_device, *tmp_peer_device;

struct gendisk *disk;

@@ -2933,7 +2933,7 @@ enum drbd_ret_code drbd_create_device(struct drbd_config_context *adm_ctx, unsig

out_idr_remove_vol:

idr_remove(&connection->peer_devices, vnr);

out_idr_remove_from_resource:

- for_each_connection(connection, resource) {

+ for_each_connection_safe(connection, n, resource) {

peer_device = idr_remove(&connection->peer_devices, vnr);

if (peer_device)

kref_put(&connection->kref, drbd_destroy_connection);