



author Jiasheng Jiang <jiasheng@iscas.ac.cn> 2023-03-16 14:55:06 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-04-05 11:16:41 +0200
commit [4a32a9a818a895671bd43e0c40351e60e4e9140b](#) (patch)
tree [b7d5ba38360b6f459a4c224d728fdbf7c780db1d](#)
parent [f8cbad984b1601435d087125ac760d3cae90213a](#) (diff)
download [linux-4a32a9a818a895671bd43e0c40351e60e4e9140b.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

dm stats: check for and propagate alloc_percpu failure

commit d3aa3e060c4a80827eb801fc448debc9daa7c46b upstream.

Check alloc_percpu()'s return value and return an error from dm_stats_init() if it fails. Update alloc_dev() to fail if dm_stats_init() does.

Otherwise, a NULL pointer dereference will occur in dm_stats_cleanup() even if dm-stats isn't being actively used.

Fixes: fd2ed4d25270 ("dm: add statistics support")

Cc: stable@vger.kernel.org

Signed-off-by: Jiasheng Jiang <jiasheng@iscas.ac.cn>

Signed-off-by: Mike Snitzer <snitzer@kernel.org>

Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

```
-rw-r--r-- drivers/md/dm-stats.c 7  
-rw-r--r-- drivers/md/dm-stats.h 2  
-rw-r--r-- drivers/md/dm.c 4
```

3 files changed, 10 insertions, 3 deletions

diff --git a/drivers/md/dm-stats.c b/drivers/md/dm-stats.c

index ce6d3bce1b7b02..0f42f4a7f38244 100644

--- a/drivers/md/dm-stats.c

+++ b/drivers/md/dm-stats.c

```
@@ -188,7 +188,7 @@ static int dm_stat_in_flight(struct dm_stat_shared *shared)  
        atomic_read(&shared->in_flight[WRITE]);  
}
```

```
-void dm_stats_init(struct dm_stats *stats)
```

```
+int dm_stats_init(struct dm_stats *stats)
```

```
{  
    int cpu;  
    struct dm_stats_last_position *last;  
@@ -196,11 +196,16 @@ void dm_stats_init(struct dm_stats *stats)  
    mutex_init(&stats->mutex);  
    INIT_LIST_HEAD(&stats->list);  
    stats->last = alloc_percpu(struct dm_stats_last_position);  
+    if (!stats->last)  
+        return -ENOMEM;  
+}
```

```

        for_each_possible_cpu(cpu) {
            last = per_cpu_ptr(stats->last, cpu);
            last->last_sector = (sector_t)ULLONG_MAX;
            last->last_rw = UINT_MAX;
        }
+
+     return 0;
+ }

void dm_stats_cleanup(struct dm_stats *stats)

diff --git a/drivers/md/dm-stats.h b/drivers/md/dm-stats.h
index 2ddfae678f320f..dcac11fce03bba 100644
--- a/drivers/md/dm-stats.h
+++ b/drivers/md/dm-stats.h
@@ -22,7 +22,7 @@ struct dm_stats_aux {
    unsigned long long duration_ns;
};

-void dm_stats_init(struct dm_stats *st);
+int dm_stats_init(struct dm_stats *st);
void dm_stats_cleanup(struct dm_stats *st);

struct mapped_device;

diff --git a/drivers/md/dm.c b/drivers/md/dm.c
index b58ff1a0fda7d1..771167ee552cde 100644
--- a/drivers/md/dm.c
+++ b/drivers/md/dm.c
@@ -1994,7 +1994,9 @@ static struct mapped_device *alloc_dev(int minor)
    if (!md->bdev)
        goto bad;

-    dm_stats_init(&md->stats);
+    r = dm_stats_init(&md->stats);
+    if (r < 0)
+        goto bad;

    /* Populate the mapping, nobody knows we exist yet */
    spin_lock(&_minor_lock);

```