



author Jiasheng Jiang <jiasheng@iscas.ac.cn> 2023-03-16 14:55:06 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-04-05 11:15:38 +0200
commit [0d96bd507ed7e7d565b6d53ebd3874686f123b2e](#) (patch)
tree [92ec0e0466eca038335aecf3121dbd3efd0d954e](#)
parent [5fc2b9485a8722c8350c3379992f5931ccfeaf98](#) (diff)
download [linux-0d96bd507ed7e7d565b6d53ebd3874686f123b2e.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 3d59f3e208c503..0eb48e739f7ea2 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 3d9a77f4e20f89..9a9b2adcf39e35 100644
```

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

```
+++ b/drivers/md/dm.c
```

```
@@ -2021,7 +2021,9 @@ static struct mapped_device *alloc_dev(int minor)
    bio_set_dev(&md->flush_bio, md->bdev);
    md->flush_bio.bi_opf = REQ_OP_WRITE | REQ_PREFLUSH | REQ_SYNC;

```

```
-    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);

```