author	Jiasheng Jiang <jiasheng@iscas.ac.cn>	2023-03-16 14:55:06 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-04-05 11:14:18 +0200
commit	2287d7b721471a3d58bcd829250336e3cdf1635e (patch)	
tree	54b3ea27d69d68c113ae8f94bebf5f845a0678ca	
parent	b8cb50c68c87f2c4a1d65df9275073e9c94aef5e (diff)	
download	linux-2287d7b721471a3d58bcd829250336e3cdf1635e.tar.gz	

diff options

context: 3

space: include

mode: unified

dm stats: check for and propagate alloc_percpu failure

```
commit d3aa3e060c4a80827eb801fc448debc9daa7c46b upstream.

Check alloc_precpu()'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 9734f506ecfd86..b72448900f5f65 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 e3facf14f61496..92f92ea417b93b 100644
--- a/drivers/md/dm.c
+++ b/drivers/md/dm.c
@@ -1799,7 +1799,9 @@ 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);
```