author	Yang Yingliang <yangyingliang@huawei.com>	2022-10-22 15:42:12 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-25 17:45:51 +0100
commit	8dddf2699da296c84205582aaead6b43dd7e8c4b (patch)	
tree	861d57d6c326254a0ce2064f35df7535dddb57aa	
parent	85d2a8b287a89853c0dcfc5a97b5e9d36376fe37 (diff)	
download	linux-8dddf2699da296c84205582aaead6b43dd7e8c4b.tar.gz	

iio: trigger: sysfs: fix possible memory leak in iio_sysfs_trig_init()

```
commit efa17e90e1711bdb084e3954fa44afb6647331c0 upstream.

dev_set_name() allocates memory for name, it need be freed
when device_add() fails, call put_device() to give up the
reference that hold in device_initialize(), so that it can
be freed in kobject_cleanup() when the refcount hit to 0.

Fault injection test can trigger this:

unreferenced object 0xffff8e8340a7b4c0 (size 32):
  comm "modprobe", pid 243, jiffies 4294678145 (age 48.845s)
  hex dump (first 32 bytes):
    69 69 6f 5f 73 79 73 66 73 5f 74 72 69 67 67 65  iio_sysfs_trigge
    72 00 a7 40 83 8e ff ff 00 86 13 c4 f6 ee ff ff  r..@............
  backtrace:
    [<0000000074999de8>] __kmem_cache_alloc_node+0x1e9/0x360
    [<00000000497fd30b>] __kmalloc_node_track_caller+0x44/0x1a0
    [<000000003636c520>] kstrdup+0x2d/0x60
    [<0000000032f84da2>] kobject_set_name_vargs+0x1e/0x90
    [<0000000092efe493>] dev_set_name+0x4e/0x70

Fixes: 1f785681a870 ("staging:iio:trigger sysfs userspace trigger rework.")
Signed-off-by: Yang Yingliang <yangyingliang@huawei.com>
Cc: <Stable@vger.kernel.org>
Link: https://lore.kernel.org/r/20221022074212.1386424-1-yangyingliang@huawei.com
Signed-off-by: Jonathan Cameron <Jonathan.Cameron@huawei.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r--	drivers/iio/trigger/iio-trig-sysfs.c	6

1 files changed, 5 insertions, 1 deletions

```
diff --git a/drivers/iio/trigger/iio-trig-sysfs.c b/drivers/iio/trigger/iio-trig-sysfs.c
index 2277d6336ac065..9ed5b9405ade0a 100644
--- a/drivers/iio/trigger/iio-trig-sysfs.c
+++ b/drivers/iio/trigger/iio-trig-sysfs.c
@@ -209,9 +209,13 @@ static int iio_sysfs_trigger_remove(int id)

 static int __init iio_sysfs_trig_init(void)
 {
```

```
+       int ret;
        device_initialize(&iio_sysfs_trig_dev);
        dev_set_name(&iio_sysfs_trig_dev, "iio_sysfs_trigger");
-       return device_add(&iio_sysfs_trig_dev);
+       ret = device_add(&iio_sysfs_trig_dev);
+       if (ret)
+               put_device(&iio_sysfs_trig_dev);
+       return ret;
 }
 module_init(iio_sysfs_trig_init);
```