author	Shang XiaoJing <shangxiaojing@huawei.com>	2022-11-02 15:29:54 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-10 18:17:33 +0100
commit	71aeb8d01a8c7ab5cf7da3f81b35206f56ce6bca (patch)	
tree	d0437ac8e8cda86f59bc38c6ac4d6e5a67b3c7cb	
parent	5c0e2da85422f22b146e42d864198df3c219c95b (diff)	
download	linux-71aeb8d01a8c7ab5cf7da3f81b35206f56ce6bca.tar.gz	

tracing: kprobe: Fix memory leak in test_gen_kprobe/kretprobe_cmd()

```
commit 66f0919c953ef7b55e5ab94389a013da2ce80a2c upstream.

test_gen_kprobe_cmd() only free buf in fail path, hence buf will leak
when there is no failure. Move kfree(buf) from fail path to common path
to prevent the memleak. The same reason and solution in
test_gen_kretprobe_cmd().

unreferenced object 0xffff888143b14000 (size 2048):
  comm "insmod", pid 52490, jiffies 4301890980 (age 40.553s)
  hex dump (first 32 bytes):
    70 3a 6b 70 72 6f 62 65 73 2f 67 65 6e 5f 6b 70  p:kprobes/gen_kp
    72 6f 62 65 5f 74 65 73 74 20 64 6f 5f 73 79 73  robe_test do_sys
  backtrace:
    [<000000006d7b836b>] kmalloc_trace+0x27/0xa0
    [<0000000009528b5b>] 0xffffffffa059006f
    [<000000008408b580>] do_one_initcall+0x87/0x2a0
    [<00000000c4980a7e>] do_init_module+0xdf/0x320
    [<00000000d775aad0>] load_module+0x3006/0x3390
    [<00000000e9a74b80>] __do_sys_finit_module+0x113/0x1b0
    [<000000003726480d>] do_syscall_64+0x35/0x80
    [<000000003441e93b>] entry_SYSCALL_64_after_hwframe+0x46/0xb0

Link: https://lore.kernel.org/all/20221102072954.26555-1-shangxiaojing@huawei.com/

Fixes: 64836248dda2 ("tracing: Add kprobe event command generation test module")
Cc: stable@vger.kernel.org
Signed-off-by: Shang XiaoJing <shangxiaojing@huawei.com>
Acked-by: Masami Hiramatsu (Google) <mhiramat@kernel.org>
Signed-off-by: Masami Hiramatsu (Google) <mhiramat@kernel.org>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r-- kernel/trace/kprobe_event_gen_test.c 18

1 files changed, 7 insertions, 11 deletions

```
diff --git a/kernel/trace/kprobe_event_gen_test.c b/kernel/trace/kprobe_event_gen_test.c
index 80e04a1e19772a..d81f7c51025c79 100644
--- a/kernel/trace/kprobe_event_gen_test.c
+++ b/kernel/trace/kprobe_event_gen_test.c
@@ -100,20 +100,20 @@ static int __init test_gen_kprobe_cmd(void)
                                       KPROBE_GEN_TEST_FUNC,
```

```
                                        KPROBE_GEN_TEST_ARG0, KPROBE_GEN_TEST_ARG1);
        if (ret)
-               goto free;
+               goto out;

        /* Use kprobe_event_add_fields to add the rest of the fields */

        ret = kprobe_event_add_fields(&cmd, KPROBE_GEN_TEST_ARG2, KPROBE_GEN_TEST_ARG3);
        if (ret)
-               goto free;
+               goto out;

        /*
         * This actually creates the event.
         */
        ret = kprobe_event_gen_cmd_end(&cmd);
        if (ret)
-               goto free;
+               goto out;

        /*
         * Now get the gen_kprobe_test event file.  We need to prevent
@@ -136,13 +136,11 @@ static int __init test_gen_kprobe_cmd(void)
                goto delete;
        }
  out:
+       kfree(buf);
        return ret;
  delete:
        /* We got an error after creating the event, delete it */
        ret = kprobe_event_delete("gen_kprobe_test");
- free:
-       kfree(buf);
-
        goto out;
 }

@@ -170,14 +168,14 @@ static int __init test_gen_kretprobe_cmd(void)
                                            KPROBE_GEN_TEST_FUNC,
                                            "$retval");
        if (ret)
-               goto free;
+               goto out;

        /*
         * This actually creates the event.
         */
        ret = kretprobe_event_gen_cmd_end(&cmd);
        if (ret)
-               goto free;
+               goto out;

        /*
         * Now get the gen_kretprobe_test event file.  We need to
@@ -201,13 +199,11 @@ static int __init test_gen_kretprobe_cmd(void)
                goto delete;
        }
  out:
+       kfree(buf);
        return ret;
  delete:
        /* We got an error after creating the event, delete it */
```

```
        ret = kprobe_event_delete("gen_kretprobe_test");
- free:
-       kfree(buf);
-
        goto out;
 }
```