



author Yi Yang <yiyang13@huawei.com> 2022-11-18 10:15:34 +0900
committer Masami Hiramatsu (Google) <mhiramat@kernel.org> 2022-11-18 10:15:34 +0900
commit [0a1ebe35cb3b7aa1f4b26b37e2a0b9ae68dc4ffb](#) (patch)
tree [5c75101639b1b9dbef0dd42fad838504a48fe19f](#)
parent [d1776c0202aac8251e6b4cbe096ad2950ed6c506](#) (diff)
download [linux-0a1ebe35cb3b7aa1f4b26b37e2a0b9ae68dc4ffb.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

rethook: fix a potential memleak in rethook_alloc()

In rethook_alloc(), the variable rh is not freed or passed out if handler is NULL, which could lead to a memleak, fix it.

Link: <https://lore.kernel.org/all/20221110104438.88099-1-yiyang13@huawei.com/>
[Masami: Add "rethook:" tag to the title.]

Fixes: 54ecbe6f1ed5 ("rethook: Add a generic return hook")
Cc: stable@vger.kernel.org
Signed-off-by: Yi Yang <yiyang13@huawei.com>
Acke-by: Masami Hiramatsu (Google) <mhiramat@kernel.org>
Signed-off-by: Masami Hiramatsu (Google) <mhiramat@kernel.org>

Diffstat

```
-rw-r--r-- kernel/trace/rethook.c 4
```

1 files changed, 3 insertions, 1 deletions

diff --git a/kernel/trace/rethook.c b/kernel/trace/rethook.c

index c69d82273ce782..32c3dfdb4d6a74 100644

--- a/kernel/trace/rethook.c

+++ b/kernel/trace/rethook.c

```
@@ -83,8 +83,10 @@ struct rethook *rethook_alloc(void *data, rethook_handler_t handler)
{
    struct rethook *rh = kzalloc(sizeof(struct rethook), GFP_KERNEL);

-    if (!rh || !handler)
+    if (!rh || !handler) {
+        kfree(rh);
+        return NULL;
+    }

    rh->data = data;
    rh->handler = handler;
```