



author Xiu Jianfeng <xiujianfeng@huawei.com> 2022-11-16 09:52:07 +0800
committer Steven Rostedt (Google) <rostedt@goodmis.org> 2022-11-17 17:16:44 -0500
commit [19ba6c8af9382c4c05dc6a0a79af3013b9a35cd0](#) (patch)
tree [4ffa27210d5f1255198cc33f42968db3396e7839](#)
parent [56f4ca0a79a9f1af98f26c54b9b89ba1f9bcc6bd](#) (diff)
download [linux-19ba6c8af9382c4c05dc6a0a79af3013b9a35cd0.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

ftrace: Fix null pointer dereference in ftrace_add_mod()

The @ftrace_mod is allocated by kzalloc(), so both the members {prev,next} of @ftrace_mod->list are NULL, it's not a valid state to call list_del(). If kstrdup() for @ftrace_mod->{func|module} fails, it goes to @out_free tag and calls free_ftrace_mod() to destroy @ftrace_mod, then list_del() will write prev->next and next->prev, where null pointer dereference happens.

BUG: kernel NULL pointer dereference, address: 0000000000000008

Oops: 0002 [#1] PREEMPT SMP NOPTI

Call Trace:

```
<TASK>
ftrace_mod_callback+0x20d/0x220
? do_filp_open+0xd9/0x140
ftrace_process_regex.isra.51+0xbfb/0x130
ftrace_regex_write.isra.52.part.53+0x6e/0x90
vfs_write+0xee/0x3a0
? __audit_filter_op+0xb1/0x100
? auditd_test_task+0x38/0x50
ksys_write+0xa5/0xe0
do_syscall_64+0x3a/0x90
entry_SYSCALL_64_after_hwframe+0x63/0xcd
Kernel panic - not syncing: Fatal exception
```

So call INIT_LIST_HEAD() to initialize the list member to fix this issue.

Link: <https://lkml.kernel.org/r/20221116015207.30858-1-xiujianfeng@huawei.com>

Cc: stable@vger.kernel.org

Fixes: 673feb9d76ab ("ftrace: Add :mod: caching infrastructure to trace_array")

Signed-off-by: Xiu Jianfeng <xiujianfeng@huawei.com>

Signed-off-by: Steven Rostedt (Google) <rostedt@goodmis.org>

Diffstat

```
-rw-r--r-- kernel/trace/ftrace.c 1
```

1 files changed, 1 insertions, 0 deletions

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

index 56a168121bfc0f..33236241f23646 100644

--- a/kernel/trace/ftrace.c

+++ b/kernel/trace/ftrace.c

@@ -1289,6 +1289,7 @@ static int ftrace_add_mod(struct trace_array *tr,

```
if (!ftrace_mod)
    return -ENOMEM;
```

```
+ INIT_LIST_HEAD(&ftrace_mod->list);
ftrace_mod->func = kstrdup(func, GFP_KERNEL);
ftrace_mod->module = kstrdup(module, GFP_KERNEL);
ftrace_mod->enable = enable;
```