



index : kernel/git/stable/linux.git

master



switch

Linux kernel stable tree

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg



search

author Eiichi Tsukata <eiichi.tsukata@nutanix.com> 2022-10-28 09:26:31 +0000
committer Paolo Bonzini <pbonzini@redhat.com> 2022-10-28 06:47:26 -0400
commit 7353633814f6e5b4899fb9ee1483709d6bb0e1cd (patch)
tree d2f9b7aba1303109482e7cad9a6b5c317d495894
parent 696db303e54f7352623d9f640e6c51d8fa9d5588 (diff)
download [linux-7353633814f6e5b4899fb9ee1483709d6bb0e1cd.tar.gz](#)

diff options

context:

3



space:

include



mode:

unified



KVM: x86/xen: Fix eventfd error handling in kvm_xen_eventfd_assign()

Should not call eventfd_ctx_put() in case of error.

Fixes: 2fd6df2f2b47 ("KVM: x86/xen: intercept EVTCHNOP_send from guests")

Reported-by: syzbot+6f0c896c5a9449a10ded@syzkaller.appspotmail.com

Signed-off-by: Eiichi Tsukata <eiichi.tsukata@nutanix.com>

Message-Id: <20221028092631.117438-1-eiichi.tsukata@nutanix.com>

[Introduce new goto target instead. - Paolo]

Signed-off-by: Paolo Bonzini <pbonzini@redhat.com>

Diffstat

-rw-r--r-- [arch/x86/kvm/xen.c](#) 7

1 files changed, 4 insertions, 3 deletions

diff --git a/arch/x86/kvm/xen.c b/arch/x86/kvm/xen.c

index b2be60c6efa4bb..2dae413bd62a65 100644

--- a/arch/x86/kvm/xen.c

+++ b/arch/x86/kvm/xen.c

```
@@ -1666,18 +1666,18 @@ static int kvm_xen_eventfd_assign(struct kvm *kvm,
     case EVTCHNSTAT_ipi:
         /* IPI must map back to the same port# */
         if (data->u.evtchn.deliver.port.port != data->u.evtchn.send_port)
-            goto out; /* -EINVAL */
+            goto out_noeventfd; /* -EINVAL */
         break;

     case EVTCHNSTAT_interdomain:
         if (data->u.evtchn.deliver.port.port) {
             if (data->u.evtchn.deliver.port.port >= max_evtchn_port(kvm))
-                goto out; /* -EINVAL */
+                goto out_noeventfd; /* -EINVAL */
         } else {
             eventfd = eventfd_ctx_fdget(data->u.evtchn.deliver.eventfd.fd);
             if (IS_ERR(eventfd)) {
                 ret = PTR_ERR(eventfd);
-                goto out;
+                goto out_noeventfd;
             }
         }
         break;

@@ -1717,6 +1717,7 @@ static int kvm_xen_eventfd_assign(struct kvm *kvm,
     out:
```

```
        if (eventfd)
            eventfd_ctx_put(eventfd);
+out_noeventfd:
    kfree(evtchnfd);
    return ret;
}
```