



author Eiichi Tsukata <eiichi.tsukata@nutanix.com> 2022-10-28 09:26:31 +0000
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-26 09:27:54 +0100
commit [d76f46f47dfde220712d1420ee5dbc546c8fc674](#) (patch)
tree [74888ff46da08f248a369fc9ddc05b31cd69c830](#)
parent [2526ac6b0f5a9b38e7e9073e37141cf78408078d](#) (diff)
download [linux-d76f46f47dfde220712d1420ee5dbc546c8fc674.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

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

commit 7353633814f6e5b4899fb9ee1483709d6bb0e1cd upstream.

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>

Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

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 cecf8299b187ba..9a1950879fc44e 100644

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

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

```
@@ -1667,18 +1667,18 @@ 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;
@@ -1718,6 +1718,7 @@ static int kvm_xen_eventfd_assign(struct kvm *kvm,
out:
    if (eventfd)
        eventfd_ctx_put(eventfd);
+out_noeventfd:
    kfree(evtchnfd);
    return ret;
}
```