



author Alexander Potapenko <glider@google.com> 2022-11-04 18:58:49 +0100
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:42:20 +0100
commit [e7061dd1fef2dfb6458cd521aef27aa66f510d31](#) (patch)
tree [7783ceb968bbd4f086fd152b65d391465a912348](#)
parent [3da7098e8ffad7be49c60d0cad0e0a83d15dc7d8](#) (diff)
download [linux-e7061dd1fef2dfb6458cd521aef27aa66f510d31.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

misc/vmw_vmci: fix an infoleak in vmci_host_do_receive_datagram()

commit e5b0d06d9b10f5f43101bd6598b076c347f9295f upstream.

`struct vmci\_event\_qp` allocated by qp_notify_peer() contains padding, which may carry uninitialized data to the userspace, as observed by KMSAN:

```
BUG: KMSAN: kernel-infoleak in instrument_copy_to_user ./include/linux/instrumented.h:121
instrument_copy_to_user ./include/linux/instrumented.h:121
_copy_to_user+0x5f/0xb0 lib/usercopy.c:33
copy_to_user ./include/linux/uaccess.h:169
vmci_host_do_receive_datagram drivers/misc/vmw_vmci/vmci_host.c:431
vmci_host_unlocked_ioctl+0x33d/0x43d0 drivers/misc/vmw_vmci/vmci_host.c:925
vfs_ioctl fs/ioctl.c:51
...
```

```
Uninit was stored to memory at:
kmemdup+0x74/0xb0 mm/util.c:131
dg_dispatch_as_host drivers/misc/vmw_vmci/vmci_datagram.c:271
vmci_datagram_dispatch+0x4f8/0xfc0 drivers/misc/vmw_vmci/vmci_datagram.c:339
qp_notify_peer+0x19a/0x290 drivers/misc/vmw_vmci/vmci_queue_pair.c:1479
qp_broker_attach drivers/misc/vmw_vmci/vmci_queue_pair.c:1662
qp_broker_alloc+0x2977/0x2f30 drivers/misc/vmw_vmci/vmci_queue_pair.c:1750
vmci_qp_broker_alloc+0x96/0xd0 drivers/misc/vmw_vmci/vmci_queue_pair.c:1940
vmci_host_do_alloc_queuepair drivers/misc/vmw_vmci/vmci_host.c:488
vmci_host_unlocked_ioctl+0x24fd/0x43d0 drivers/misc/vmw_vmci/vmci_host.c:927
...
```

```
Local variable ev created at:
qp_notify_peer+0x54/0x290 drivers/misc/vmw_vmci/vmci_queue_pair.c:1456
qp_broker_attach drivers/misc/vmw_vmci/vmci_queue_pair.c:1662
qp_broker_alloc+0x2977/0x2f30 drivers/misc/vmw_vmci/vmci_queue_pair.c:1750
```

```
Bytes 28-31 of 48 are uninitialized
Memory access of size 48 starts at ffff888035155e00
Data copied to user address 0000000020000100
```

Use memset() to prevent the infoleaks.

Also speculatively fix qp_notify_peer_local(), which may suffer from the same problem.

Reported-by: syzbot+39be4da489ed2493ba25@syzkaller.appspotmail.com
Cc: stable <stable@kernel.org>
Fixes: 06164d2b72aa ("VMCI: queue pairs implementation.")
Signed-off-by: Alexander Potapenko <glider@google.com>
Reviewed-by: Vishnu Dasa <vdasa@vmware.com>
Link: <https://lore.kernel.org/r/20221104175849.2782567-1-glider@google.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

Diffstat

```
-rw-r--r-- drivers/misc/vmw_vmci/vmci_queue_pair.c 2
```

1 files changed, 2 insertions, 0 deletions

```
diff --git a/drivers/misc/vmw_vmci/vmci_queue_pair.c b/drivers/misc/vmw_vmci/vmci_queue_pair.c
index a49782dd903cd4..d4d388f021ccd8 100644
--- a/drivers/misc/vmw_vmci/vmci_queue_pair.c
+++ b/drivers/misc/vmw_vmci/vmci_queue_pair.c
@@ -852,6 +852,7 @@ static int qp_notify_peer_local(bool attach, struct vmci_handle handle)
     u32 context_id = vmci_get_context_id();
     struct vmci_event_qp ev;

+    memset(&ev, 0, sizeof(ev));
     ev.msg.hdr.dst = vmci_make_handle(context_id, VMCI_EVENT_HANDLER);
     ev.msg.hdr.src = vmci_make_handle(VMCI_HYPERVISOR_CONTEXT_ID,
                                     VMCI_CONTEXT_RESOURCE_ID);
@@ -1465,6 +1466,7 @@ static int qp_notify_peer(bool attach,
     * kernel.
     */

+    memset(&ev, 0, sizeof(ev));
     ev.msg.hdr.dst = vmci_make_handle(peer_id, VMCI_EVENT_HANDLER);
     ev.msg.hdr.src = vmci_make_handle(VMCI_HYPERVISOR_CONTEXT_ID,
                                     VMCI_CONTEXT_RESOURCE_ID);
```