Date: Wed, 22 Jun 2022 12:11:00 +0800 (GMT+08:00)
From: kangel <22021034@....edu.cn>
To: oss-security@...ts.openwall.com
Cc: secalert@...hat.com, pbonzini@...hat.com, seanjc@...gle.com,
vkuznets@...hat.com, wanpengli@...cent.com, pgn@....edu.cn,
gregkh@...uxfoundation.org
Subject: CVE-2022-2153: Linux Kernel: x86/kvm: NULL pointer dereference in
kvm_irq_delivery_to_apic_fast

------------[Description]------------ We found a 'general protection fault in kvm_irq_delivery_to_apic_fast' bug by syzkaller. The linux kernel version is 5.17.0-rc8. When KVM initialized a vCPU without create apic, the value of vcpu->arch.apic is NULL, then if we enter guest and let KVM call kvm_hv_process_stimers() in arch/x86/kvm/x86.c:9947, which not check if apic in kernel. Process stimer will use apic finally so it will cause a null pointer dereference. This flaw allows a malicious user in a Local DOS condition. The following program triggers Local DOS in kvm_irq_delivery_to_apic_fast in arch/x86/kvm/lapic.c:995, this bug can be reproducible stably by the C reproducer This bug was disclosed on March 25 and assigned CVE-2022-2153. ------------[Credits]-------
-----Yongkang Jia (Zhejiang University)Gaoning Pan (Zhejiang University)------------[Backtrace]----------
--Syzkaller hit 'general protection fault in kvm_irq_delivery_to_apic_fast' bug.

```
general protection fault, probably for non-canonical address 0xdfffffc0000000013: 0000 [#1] PREEMPT SMP
KASAN NOPTI
KASAN: null-ptr-deref in range [0x0000000000000098-0x000000000000009f]
CPU: 1 PID: 679 Comm: syz-executor210 Not tainted 5.17.0-rc8 #6
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.2-1ubuntu1~cloud0 04/01/2014
RIP: 0010:kvm_irq_delivery_to_apic_fast+0x3dd/0x670 arch/x86/kvm/lapic.c:995
Code: e9 71 fe ff ff e8 93 3f 44 00 48 8b 9c 24 88 00 00 00 48 b8 00 00 00 00 00 fc ff df 48 8d bb 98 00 00
00 48 89 fa 48 c1 ea 03 <80> 3c 02 00 0f 85 18 02 00 00 48 8b 9b 98 00 00 00 48 b8 00 00 00
RSP: 0018:ffff8880094276c0 EFLAGS: 00010202
RAX: dfffffc0000000000 RBX: 0000000000000000 RCX: ffffffff9792d12d
RDX: 0000000000000013 RSI: 0000000000000000 RDI: 0000000000000098
RBP: ffff8880094279a8 R08: 0000000000000000 R09: ffff8880094279b0
R10: ffff8880094279bf R11: ffffed1001284f37 R12: ffffc9000085d000
R13: ffff888009427858 R14: 0000000000000000 R15: 0000000000000000
FS:  00007f942fa80700(0000) GS:ffff88806d300000(0000) knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000020fe8000 CR3: 000000000852e006 CR4: 00000000003726e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400
Call Trace:
 <TASK>
 kvm_irq_delivery_to_apic+0xb8/0x860 arch/x86/kvm/irq_comm.c:54
 synic_set_irq+0x169/0x340 arch/x86/kvm/hyperv.c:463
 synic_deliver_msg arch/x86/kvm/hyperv.c:770 [inline]
 stimer_send_msg arch/x86/kvm/hyperv.c:793 [inline]
 stimer_expiration arch/x86/kvm/hyperv.c:817 [inline]
 kvm_hv_process_stimers+0xe85/0x1210 arch/x86/kvm/hyperv.c:849
 vcpu_enter_guest+0x37cb/0x4070 arch/x86/kvm/x86.c:9947
 vcpu_run arch/x86/kvm/x86.c:10261 [inline]
 kvm_arch_vcpu_ioctl_run+0x3a6/0x1670 arch/x86/kvm/x86.c:10471
 kvm_vcpu_ioctl+0x4cc/0xc70 arch/x86/kvm/../../../virt/kvm/kvm_main.c:3908
 vfs_ioctl fs/ioctl.c:51 [inline]
 __do_sys_ioctl fs/ioctl.c:874 [inline]
 __se_sys_ioctl fs/ioctl.c:860 [inline]
 __x64_sys_ioctl+0x16d/0x1d0 fs/ioctl.c:860
 do_syscall_x64 arch/x86/entry/common.c:50 [inline]
 do_syscall_64+0x38/0x90 arch/x86/entry/common.c:80
 entry_SYSCALL_64_after_hwframe+0x44/0xae
RIP: 0033:0x448b29
Code: e8 ec e7 ff ff 48 83 c4 18 c3 0f 1f 80 00 00 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89
c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 0f 83 9b fe fb ff c3 66 2e 0f 1f 84 00 00 00 00
RSP: 002b:00007f942fa7fda8 EFLAGS: 00000246 ORIG_RAX: 0000000000000010
RAX: ffffffffffffffda RBX: 00000000006ddc40 RCX: 0000000000448b29
RDX: 0000000000000000 RSI: 000000000000ae80 RDI: 0000000000000005
RBP: 00000000006ddc48 R08: 0000000000000000 R09: 0000000000000000
```

R10: 0000000000000000 R11: 0000000000000246 R12: 00000000006ddc4c
R13: 6d766b2f7665642f R14: 00007f942fa809c0 R15: 0000000000000000------------[Patch]------------The patch is public and it can be found here:https://git.kernel.org/pub/scm/virt/kvm/kvm.git/commit/?h=queue&id=00b5f37189d24ac3ed46cb7f11742094778c46ceC repro is attached.Best regards.   Yongkang Jia

Content of type "text/html**" skipped**

View attachment "poc.c**" of type "**text/plain**" (40075 bytes)**

Download attachment "config**" of type "**application/octet-stream**" (130207 bytes)**