

net tipc:fix a kernel-infoleak in __tipc_sendmsg()

[Browse files](#)

struct tipc_socket_addr.ref has a 4-byte hole, and __tipc_getname() currently copying it to user space, causing kernel-infoleak.

BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline]
BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:121 [inline]
lib/usercopy.c:33

BUG: KMSAN: kernel-infoleak in _copy_to_user+0x1c9/0x270 lib/usercopy.c:33 lib/usercopy.c:33
instrument_copy_to_user include/linux/instrumented.h:121 [inline]
instrument_copy_to_user include/linux/instrumented.h:121 [inline] lib/usercopy.c:33
_copy_to_user+0x1c9/0x270 lib/usercopy.c:33 lib/usercopy.c:33
copy_to_user include/linux/uaccess.h:209 [inline]
copy_to_user include/linux/uaccess.h:209 [inline] net/socket.c:287
move_addr_to_user+0x3f6/0x600 net/socket.c:287 net/socket.c:287
__sys_getpeername+0x470/0x6b0 net/socket.c:1987 net/socket.c:1987
__do_sys_getpeername net/socket.c:1997 [inline]
__se_sys_getpeername net/socket.c:1994 [inline]
__do_sys_getpeername net/socket.c:1997 [inline] net/socket.c:1994
__se_sys_getpeername net/socket.c:1994 [inline] net/socket.c:1994
__x64_sys_getpeername+0xda/0x120 net/socket.c:1994 net/socket.c:1994
do_syscall_x64 arch/x86/entry/common.c:51 [inline]
do_syscall_x64 arch/x86/entry/common.c:51 [inline] arch/x86/entry/common.c:82
do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 arch/x86/entry/common.c:82
entry_SYSCALL_64_after_hwframe+0x44/0xae

Uninit was stored to memory at:

tipc_getname+0x575/0x5e0 net/tipc/socket.c:757 net/tipc/socket.c:757
__sys_getpeername+0x3b3/0x6b0 net/socket.c:1984 net/socket.c:1984
__do_sys_getpeername net/socket.c:1997 [inline]
__se_sys_getpeername net/socket.c:1994 [inline]
__do_sys_getpeername net/socket.c:1997 [inline] net/socket.c:1994
__se_sys_getpeername net/socket.c:1994 [inline] net/socket.c:1994
__x64_sys_getpeername+0xda/0x120 net/socket.c:1994 net/socket.c:1994
do_syscall_x64 arch/x86/entry/common.c:51 [inline]
do_syscall_x64 arch/x86/entry/common.c:51 [inline] arch/x86/entry/common.c:82
do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 arch/x86/entry/common.c:82
entry_SYSCALL_64_after_hwframe+0x44/0xae

Uninit was stored to memory at:

msg_set_word net/tipc/msg.h:212 [inline]
msg_set_destport net/tipc/msg.h:619 [inline]
msg_set_word net/tipc/msg.h:212 [inline] net/tipc/socket.c:1486
msg_set_destport net/tipc/msg.h:619 [inline] net/tipc/socket.c:1486
__tipc_sendmsg+0x44fa/0x5890 net/tipc/socket.c:1486 net/tipc/socket.c:1486

```
tipc_sendmsg+0xeb/0x140 net/tipc/socket.c:1402 net/tipc/socket.c:1402
sock_sendmsg_nosec net/socket.c:704 [inline]
sock_sendmsg net/socket.c:724 [inline]
sock_sendmsg_nosec net/socket.c:704 [inline] net/socket.c:2409
sock_sendmsg net/socket.c:724 [inline] net/socket.c:2409
__sys_sendmsg+0xe11/0x12c0 net/socket.c:2409 net/socket.c:2409
__sys_sendmsg net/socket.c:2463 [inline]
__sys_sendmsg net/socket.c:2463 [inline] net/socket.c:2492
__sys_sendmsg+0x704/0x840 net/socket.c:2492 net/socket.c:2492
__do_sys_sendmsg net/socket.c:2501 [inline]
__se_sys_sendmsg net/socket.c:2499 [inline]
__do_sys_sendmsg net/socket.c:2501 [inline] net/socket.c:2499
__se_sys_sendmsg net/socket.c:2499 [inline] net/socket.c:2499
__x64_sys_sendmsg+0xe2/0x120 net/socket.c:2499 net/socket.c:2499
do_syscall_x64 arch/x86/entry/common.c:51 [inline]
do_syscall_x64 arch/x86/entry/common.c:51 [inline] arch/x86/entry/common.c:82
do_syscall_64+0x54/0xd0 arch/x86/entry/common.c:82 arch/x86/entry/common.c:82
entry_SYSCALL_64_after_hwframe+0x44/0xae
```

Local variable skaddr created at:

```
__tipc_sendmsg+0x2d0/0x5890 net/tipc/socket.c:1419 net/tipc/socket.c:1419
tipc_sendmsg+0xeb/0x140 net/tipc/socket.c:1402 net/tipc/socket.c:1402
```

Bytes 4-7 of 16 are uninitialized

Memory access of size 16 starts at ffff888113753e00

Data copied to user address 0000000020000280

Reported-by: syzbot+cdbd40e0c3ca02cae3b7@syzkaller.appspotmail.com

Signed-off-by: Haimin Zhang <tcs_kernel@tencent.com>


Acked-by: Jon Maloy <jmaloy@redhat.com>

Link: <https://lore.kernel.org/r/1640918123-14547-1-git-send-email-tcs.kernel@gmail.com>

Signed-off-by: Jakub Kicinski <kuba@kernel.org>

 master

 v6.1-rc6 ... v5.16

 YunDingLab authored and kuba-moo committed on Dec 31

1 parent 5e75d0b commit d6d86830705f173fca6087a3e67ceaf68db80523

Showing 1 changed file with 2 additions and 0 deletions.

Split

Unified

▼ ↕ 2 ■■■ net/tipc/socket.c 

1461	1461		msg_set_syn(hdr, 1);
1462	1462		}
1463	1463		
	1464	+	memset(&skaddr, 0, sizeof(skaddr));
	1465	+	
1464	1466		/* Determine destination */

1465	1467	<code>if (atype == TIPC_SERVICE_RANGE) {</code>
1466	1468	<code>return tipc_sendmcast(sock, ua, m, dlen, timeout);</code>

0 comments on commit d6d8683

Please [sign in](#) to comment.