author	Alexandra Winter <wintera@linux.ibm.com>	2023-03-15 14:14:35 +0100
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-03-22 13:31:28 +0100
commit	3cfdefdaaa4b2a77e84d0db5e0a47a7aa3bb615a (patch)	
tree	6b2f3a5ed2c25b458f5bc9c438f22ead85888429	
parent	7bf0eac3fdd2d25f5c6ceab63e3e4902e274f7ee (diff)	
download	linux-3cfdefdaaa4b2a77e84d0db5e0a47a7aa3bb615a.tar.gz	

net/iucv: Fix size of interrupt data

```
[ Upstream commit 3d87debb8ed2649608ff432699e7c961c0c6f03b ]

iucv_irq_data needs to be 4 bytes larger.
These bytes are not used by the iucv module, but written by
the z/VM hypervisor in case a CPU is deconfigured.

Reported as:
BUG dma-kmalloc-64 (Not tainted): kmalloc Redzone overwritten
-----------------------------------------------------------------------------
0x0000000000400564-0x0000000000400567 @offset=1380. First byte 0x80 instead of 0xcc
Allocated in iucv_cpu_prepare+0x44/0xd0 age=167839 cpu=2 pid=1
__kmem_cache_alloc_node+0x166/0x450
kmalloc_node_trace+0x3a/0x70
iucv_cpu_prepare+0x44/0xd0
cpuhp_invoke_callback+0x156/0x2f0
cpuhp_issue_call+0xf0/0x298
__cpuhp_setup_state_cpuslocked+0x136/0x338
__cpuhp_setup_state+0xf4/0x288
iucv_init+0xf4/0x280
do_one_initcall+0x78/0x390
do_initcalls+0x11a/0x140
kernel_init_freeable+0x25e/0x2a0
kernel_init+0x2e/0x170
__ret_from_fork+0x3c/0x58
ret_from_fork+0xa/0x40
Freed in iucv_init+0x92/0x280 age=167839 cpu=2 pid=1
__kmem_cache_free+0x308/0x358
iucv_init+0x92/0x280
do_one_initcall+0x78/0x390
do_initcalls+0x11a/0x140
kernel_init_freeable+0x25e/0x2a0
kernel_init+0x2e/0x170
__ret_from_fork+0x3c/0x58
ret_from_fork+0xa/0x40
Slab 0x0000037200010000 objects=32 used=30 fp=0x0000000000400640 flags=0x1ffff00000010200(slab|head|node=0|zone=0|
Object 0x0000000000400540 @offset=1344 fp=0x0000000000000000
Redzone  0000000000400500: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  ................
Redzone  0000000000400510: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  ................
Redzone  0000000000400520: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  ................
Redzone  0000000000400530: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  ................
Object   0000000000400540: 00 01 00 03 00 00 00 00 00 00 00 00 00 00 00 00  ................
Object   0000000000400550: f3 86 81 f2 f4 82 f8 82 f0 f0 f0 f0 f0 f0 f0 f2  ................
Object   0000000000400560: 00 00 00 00 80 00 00 00 cc cc cc cc cc cc cc cc  ................
Object   0000000000400570: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  ................
Redzone  0000000000400580: cc cc cc cc cc cc cc cc                          ........
Padding  00000000004005d4: 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a  ZZZZZZZZZZZZZZZZ
Padding  00000000004005e4: 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a  ZZZZZZZZZZZZZZZZ
Padding  00000000004005f4: 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a 5a              ZZZZZZZZZZZZ
CPU: 6 PID: 121030 Comm: 116-pai-crypto. Not tainted 6.3.0-20230221.rc0.git4.99b8246b2d71.300.fc37.s390x+debug #1
Hardware name: IBM 3931 A01 704 (z/VM 7.3.0)
Call Trace:
[<000000032aa034ec>] dump_stack_lvl+0xac/0x100
```

```
[<0000000329f5a6cc>] check_bytes_and_report+0x104/0x140
[<0000000329f5aa78>] check_object+0x370/0x3c0
[<0000000329f5ede6>] free_debug_processing+0x15e/0x348
[<0000000329f5f06a>] free_to_partial_list+0x9a/0x2f0
[<0000000329f5f4a4>] __slab_free+0x1e4/0x3a8
[<0000000329f61768>] __kmem_cache_free+0x308/0x358
[<000000032a91465c>] iucv_cpu_dead+0x6c/0x88
[<0000000329c2fc66>] cpuhp_invoke_callback+0x156/0x2f0
[<000000032aa062da>] _cpu_down.constprop.0+0x22a/0x5e0
[<0000000329c3243e>] cpu_device_down+0x4e/0x78
[<000000032a61dee0>] device_offline+0xc8/0x118
[<000000032a61e048>] online_store+0x60/0xe0
[<000000032a08b6b0>] kernfs_fop_write_iter+0x150/0x1e8
[<0000000329fab65c>] vfs_write+0x174/0x360
[<0000000329fab9fc>] ksys_write+0x74/0x100
[<000000032aa03a5a>] __do_syscall+0x1da/0x208
[<000000032aa177b2>] system_call+0x82/0xb0
INFO: lockdep is turned off.
FIX dma-kmalloc-64: Restoring kmalloc Redzone 0x0000000000400564-0x0000000000400567=0xcc
FIX dma-kmalloc-64: Object at 0x0000000000400540 not freed

Fixes: 2356f4cb1911 ("[S390]: Rewrite of the IUCV base code, part 2")
Signed-off-by: Alexandra Winter <wintera@linux.ibm.com>
Link: https://lore.kernel.org/r/20230315131435.4113889-1-wintera@linux.ibm.com
Signed-off-by: Jakub Kicinski <kuba@kernel.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- net/iucv/iucv.c 2

1 files changed, 1 insertions, 1 deletions

```
diff --git a/net/iucv/iucv.c b/net/iucv/iucv.c
index f3343a8541a57e..8efc369934fc7d 100644
--- a/net/iucv/iucv.c
+++ b/net/iucv/iucv.c
@@ -83,7 +83,7 @@ struct iucv_irq_data {
        u16 ippathid;
        u8  ipflags1;
        u8  iptype;
-       u32 res2[8];
+       u32 res2[9];
 };

 struct iucv_irq_list {
```