



author Dan Williams <dan.j.williams@intel.com> 2022-11-03 17:30:24 -0700
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 18:17:32 +0100
commit [12316b9f7c18138ae656050cfd716728e27b7e2f](#) (patch)
tree [431e5e906e7a09bea8a74927d11998eb89a0814c](#)
parent [c6813b5610ac53af73edd87a660d23a0511faa47](#) (diff)
download [linux-12316b9f7c18138ae656050cfd716728e27b7e2f.tar.gz](#)

diff options

context:
space:
mode:

cxl/region: Fix region HPA ordering validation

commit a90accb358ae33ea982a35595573f7a045993f8b upstream.

Some regions may not have any address space allocated. Skip them when validating HPA order otherwise a crash like the following may result:

```
devm_cxl_add_region: cxl_acpi cxl_acpi.0: decoder3.4: created region9
BUG: kernel NULL pointer dereference, address: 0000000000000000
[...]
```

RIP: 0010:store_targetN+0x655/0x1740 [cxl_core]

[...]

Call Trace:

<TASK>

kernfs_fop_write_iter+0x144/0x200

vfs_write+0x24a/0x4d0

ksys_write+0x69/0xf0

do_syscall_64+0x3a/0x90

```
store_targetN+0x655/0x1740:
alloc_region_ref at drivers/cxl/core/region.c:676
(inlined by) cxl_port_attach_region at drivers/cxl/core/region.c:850
(inlined by) cxl_region_attach at drivers/cxl/core/region.c:1290
(inlined by) attach_target at drivers/cxl/core/region.c:1410
(inlined by) store_targetN at drivers/cxl/core/region.c:1453
```

Cc: <stable@vger.kernel.org>

Fixes: 384e624bb211 ("cxl/region: Attach endpoint decoders")

Reviewed-by: Vishal Verma <vishal.l.verma@intel.com>

Reviewed-by: Dave Jiang <dave.jiang@intel.com>

Link: <https://lore.kernel.org/r/166752182461.947915.497032805239915067.stgit@dwillia2-xfh.jf.intel.com>

Signed-off-by: Dan Williams <dan.j.williams@intel.com>

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

Diffstat

```
-rw-r--r-- drivers/cxl/core/region.c 3
```

1 files changed, 3 insertions, 0 deletions

diff --git a/drivers/cxl/core/region.c b/drivers/cxl/core/region.c

index 986855e93e7144..80dd9608324cc3 100644

--- a/drivers/cxl/core/region.c

+++ b/drivers/cxl/core/region.c

```
@@ -657,6 +657,9 @@ static struct cxl_region_ref *alloc_region_ref(struct cxl_port *port,
     xa_for_each(&port->regions, index, iter) {
         struct cxl_region_params *ip = &iter->region->params;
```

```
+      if (!ip->res)
+          continue;
+
+      if (ip->res->start > p->res->start) {
+          dev_dbg(&cxlr->dev,
+              "%s: HPA order violation %s:%pr vs %pr\n",
```