author	Thomas Richter <tmricht@linux.ibm.com>	2025-04-09 10:03:53 +0200
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2025-04-20 10:18:29 +0200
commit	3a3faf873db5dcd5d2622d8e2accb90af0a86c2d (patch)	
tree	ea5b0fa91d61a0321860cb37ce3c0752b2fd95d7	
parent	8e5aff600539e5faea294d9612cca50220e602b8 (diff)	
download	linux-3a3faf873db5dcd5d2622d8e2accb90af0a86c2d.tar.gz	

diff options

context: 3

space: include

mode: unified

s390/cpumf: Fix double free on error in cpumf_pmu_event_init()

```
commit aa1ac98268cd1f380c713f07e39b1fa1d5c7650c upstream.

In PMU event initialization functions
 - cpumsf_pmu_event_init()
 - cpumf_pmu_event_init()
 - cfdiag_event_init()
the partially created event had to be removed when an error was detected.
The event::event_init() member function had to release all resources
it allocated in case of error. event::destroy() had to be called
on freeing an event after it was successfully created and
event::event_init() returned success.

With

commit c70ca298036c ("perf/core: Simplify the perf_event_alloc() error path")

this is not necessary anymore. The performance subsystem common
code now always calls event::destroy() to clean up the allocated
resources created during event initialization.

Remove the event::destroy() invocation in PMU event initialization
or that function is called twice for each event that runs into an
error condition in event creation.

This is the kernel log entry which shows up without the fix:

------------[ cut here ]------------
refcount_t: underflow; use-after-free.
WARNING: CPU: 0 PID: 43388 at lib/refcount.c:87 refcount_dec_not_one+0x74/0x90
CPU: 0 UID: 0 PID: 43388 Comm: perf Not tainted 6.15.0-20250407.rc1.git0.300.fc41.s390x+git #1 NONE
Hardware name: IBM 3931 A01 704 (LPAR)
Krnl PSW : 0704c00180000000 00000209cb2c1b88 (refcount_dec_not_one+0x78/0x90)
           R:0 T:1 IO:1 EX:1 Key:0 M:1 W:0 P:0 AS:3 CC:0 PM:0 RI:0 EA:3
Krnl GPRS: 0000020900000027 0000020900000023 0000000000000026 0000018900000000
           00000004a2200a00 0000000000000000 0000000000000057 fffffffffffffea
           00000002b386c600 00000002b3f5b3e0 00000209cc51f140 00000209cc7fc550
           0000000001449d38 ffffffffffffffff 00000209cb2c1b84 00000189d67dfb80
Krnl Code: 00000209cb2c1b78: c02000506727       larl    %r2,00000209cbcce9c6
           00000209cb2c1b7e: c0e5ffbd4431       brasl   %r14,00000209caa6a3e0
          #00000209cb2c1b84: af000000           mc      0,0
          >00000209cb2c1b88: a7480001           lhi     %r4,1
           00000209cb2c1b8c: ebeff0a00004       lmg     %r14,%r15,160(%r15)
           00000209cb2c1b92: ec243fbf0055       risbg   %r2,%r4,63,191,0
```

```
           00000209cb2c1b98: 07fe               bcr     15,%r14
           00000209cb2c1b9a: 47000700           bc      0,1792
Call Trace:
 [<00000209cb2c1b88>] refcount_dec_not_one+0x78/0x90
 [<00000209cb2c1dc4>] refcount_dec_and_mutex_lock+0x24/0x90
 [<00000209caa3c29e>] hw_perf_event_destroy+0x2e/0x80
 [<00000209cacaf8b4>] __free_event+0x74/0x270
 [<00000209cacb47c4>] perf_event_alloc.part.0+0x4a4/0x730
 [<00000209cacbf3e8>] __do_sys_perf_event_open+0x248/0xc20
 [<00000209cacc14a4>] __s390x_sys_perf_event_open+0x44/0x50
 [<00000209cb8114de>] __do_syscall+0x12e/0x260
 [<00000209cb81ce34>] system_call+0x74/0x98
Last Breaking-Event-Address:
 [<00000209caa6a4d2>] __warn_printk+0xf2/0x100
---[ end trace 0000000000000000 ]---

Fixes: c70ca298036c ("perf/core: Simplify the perf_event_alloc() error path")
Signed-off-by: Thomas Richter <tmricht@linux.ibm.com>
Reviewed-by: Sumanth Korikkar <sumanthk@linux.ibm.com>
Signed-off-by: Heiko Carstens <hca@linux.ibm.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r--	arch/s390/kernel/perf_cpum_cf.c 9
-rw-r--r--	arch/s390/kernel/perf_cpum_sf.c 3

2 files changed, 1 insertions, 11 deletions

```
diff --git a/arch/s390/kernel/perf_cpum_cf.c b/arch/s390/kernel/perf_cpum_cf.c
index 33205dd410e470..60a60185b1d4db 100644
--- a/arch/s390/kernel/perf_cpum_cf.c
+++ b/arch/s390/kernel/perf_cpum_cf.c
@@ -858,18 +858,13 @@ static int cpumf_pmu_event_type(struct perf_event *event)
 static int cpumf_pmu_event_init(struct perf_event *event)
 {
        unsigned int type = event->attr.type;
-       int err;
+       int err = -ENOENT;

        if (type == PERF_TYPE_HARDWARE || type == PERF_TYPE_RAW)
                err = __hw_perf_event_init(event, type);
        else if (event->pmu->type == type)
                /* Registered as unknown PMU */
                err = __hw_perf_event_init(event, cpumf_pmu_event_type(event));
-       else
-               return -ENOENT;
-
-       if (unlikely(err) && event->destroy)
-               event->destroy(event);

        return err;
 }
@@ -1819,8 +1814,6 @@ static int cfdiag_event_init(struct perf_event *event)
        event->destroy = hw_perf_event_destroy;

        err = cfdiag_event_init2(event);
-       if (unlikely(err))
-               event->destroy(event);
 out:
        return err;
 }
```

```
diff --git a/arch/s390/kernel/perf_cpum_sf.c b/arch/s390/kernel/perf_cpum_sf.c
index 1e99514fb7ae3d..eb470d9a528254 100644
--- a/arch/s390/kernel/perf_cpum_sf.c
+++ b/arch/s390/kernel/perf_cpum_sf.c
@@ -885,9 +885,6 @@ static int cpumsf_pmu_event_init(struct perf_event *event)
                event->attr.exclude_idle = 0;

        err = __hw_perf_event_init(event);
-       if (unlikely(err))
-               if (event->destroy)
-                       event->destroy(event);
        return err;
 }
```