



index : kernel/git/stable/linux.git

master



switch

Linux kernel stable tree

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg



search

author Yang Jihong <yangjihong1@huawei.com> 2023-03-14 04:47:35 +0000
committer Peter Zijlstra <peterz@infradead.org> 2023-03-15 21:49:46 +0100
commit [eb81a2ed4f52be831c9fb879752d89645a312c13](#) (patch)
tree [99f2027257b3362f2d06b8e46312d1b5a2922b6b](#)
parent [eeac8ede17557680855031c6f305ece2378af326](#) (diff)
download [linux-eb81a2ed4f52be831c9fb879752d89645a312c13.tar.gz](#)

diff options

context:

3

space:

include

mode:

unified

perf/core: Fix perf_output_begin parameter is incorrectly invoked in perf_event_bpf_output

syzkaller reportes a KASAN issue with stack-out-of-bounds.
The call trace is as follows:

```
dump_stack+0x9c/0xd3
print_address_description.constprop.0+0x19/0x170
__kasan_report.cold+0x6c/0x84
kasan_report+0x3a/0x50
__perf_event_header__init_id+0x34/0x290
perf_event_header__init_id+0x48/0x60
perf_output_begin+0x4a4/0x560
perf_event_bpf_output+0x161/0x1e0
perf_iterate_sb_cpu+0x29e/0x340
perf_iterate_sb+0x4c/0xc0
perf_event_bpf_event+0x194/0x2c0
__bpf_prog_put.constprop.0+0x55/0xf0
__cls_bpf_delete_prog+0xea/0x120 [cls_bpf]
cls_bpf_delete_prog_work+0x1c/0x30 [cls_bpf]
process_one_work+0x3c2/0x730
worker_thread+0x93/0x650
kthread+0x1b8/0x210
ret_from_fork+0x1f/0x30
```

commit 267fb27352b6 ("perf: Reduce stack usage of perf_output_begin()")
use on-stack struct perf_sample_data of the caller function.

However, perf_event_bpf_output uses incorrect parameter to convert
small-sized data (struct perf_bpf_event) into large-sized data
(struct perf_sample_data), which causes memory overwriting occurs in
__perf_event_header__init_id.

Fixes: 267fb27352b6 ("perf: Reduce stack usage of perf_output_begin()")
Signed-off-by: Yang Jihong <yangjihong1@huawei.com>
Signed-off-by: Peter Zijlstra (Intel) <peterz@infradead.org>
Link: <https://lkml.kernel.org/r/20230314044735.56551-1-yangjihong1@huawei.com>

Diffstat

-rw-r--r-- [kernel/events/core.c](#) 2

1 files changed, 1 insertions, 1 deletions

diff --git a/kernel/events/core.c b/kernel/events/core.c
index f79fd8b87f75ed..296617edbd1cc 100644

--- a/kernel/events/core.c

+++ b/kernel/events/core.c

@@ -9187,7 +9187,7 @@ static void perf_event_bpf_output(struct perf_event *event, void *data)

```
    perf_event_header__init_id(&bpf_event->event_id.header,  
                               &sample, event);
```

- ret = perf_output_begin(&handle, data, event,

+ ret = perf_output_begin(&handle, &sample, event,
 bpf_event->event_id.header.size);

```
    if (ret)
```

```
        return;
```