KMSAN: kernel-infoleak in copy_page_to_iter (2)

Status: fixed on 2021/11/10 00:50
Reported-by: syzbot+2dcfeaf8cb49b05e8f1a@syzkaller.appspotmail.com
Fix commit: ce3aba43599f ext4: fix kernel infoleak via ext4_extent_header
First crash: 1610d, last: 477d

similar bugs (2):

Kernel	Title	Repro	Cause bisect	Fix bisect	Count	Last	Reported	Patched	Statu
upstream	KMSAN: kernel-infoleak in copy_page_to_iter	C			364	1611d	1632d	0/24	closed as invalid on 201
upstream	KMSAN: kernel-infoleak in copy_page_to_iter (3)				2	363d	365d	0/24	auto-closed as invalid or

Patch testing requests:

Created	Duration	User	Patch	Repo	Result
2020/09/30 17:18	18m	anant.thazhemadam@gmail.com	patch	https://github.…	report log

Sample crash report:

```
IPv6: ADDRCONF(NETDEV_UP): veth1: link is not ready
IPv6: ADDRCONF(NETDEV_CHANGE): veth1: link becomes ready
IPv6: ADDRCONF(NETDEV_CHANGE): veth0: link becomes ready
8021q: adding VLAN 0 to HW filter on device team0
==========================================================
BUG: KMSAN: kernel-infoleak in copyout lib/iov_iter.c:140 [inline]
BUG: KMSAN: kernel-infoleak in copy_page_to_iter_iovec lib/iov_iter.c:212 [inline]
BUG: KMSAN: kernel-infoleak in copy_page_to_iter+0x77a/0x1ac0 lib/iov_iter.c:846
CPU: 0 PID: 5005 Comm: blkid Not tainted 4.19.0-rc1+ #39
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
Call Trace:
 __dump_stack lib/dump_stack.c:77 [inline]
 dump_stack+0x14b/0x190 lib/dump_stack.c:113
 kmsan_report+0x183/0x2b0 mm/kmsan/kmsan.c:956
 kmsan_internal_check_memory+0x17e/0x1f0 mm/kmsan/kmsan.c:1020
 kmsan_copy_to_user+0x73/0xb0 mm/kmsan/kmsan_hooks.c:479
 copyout lib/iov_iter.c:140 [inline]
 copy_page_to_iter_iovec lib/iov_iter.c:212 [inline]
 copy_page_to_iter+0x77a/0x1ac0 lib/iov_iter.c:846
 generic_file_buffered_read mm/filemap.c:2185 [inline]
 generic_file_read_iter+0x3469/0x4430 mm/filemap.c:2362
 blkdev_read_iter+0x20d/0x270 fs/block_dev.c:1936
 call_read_iter include/linux/fs.h:1801 [inline]
 new_sync_read fs/read_write.c:406 [inline]
```

Crashes (2099):

Manager	Time	Kernel	Commit	Syzkaller	Config	Log	Report	Syz repro	C repro	VM info	
ci-upstream-kmsan-gce	2018/08/31 16:47	https://github.…	ab98bd30a4ba	a4718693	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/08/30 12:57	https://github.…	2dca2cbde67a	6c7e9d3d	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/08/30 11:32	https://github.…	2dca2cbde67a	6c7e9d3d	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/08/25 03:09	https://github.…	0cc51dc9a291	9b0f5c75	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/08/25 01:57	https://github.…	0cc51dc9a291	9b0f5c75	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/23 10:46	https://github.…	d1c2a46a46f6	f69c5fcd	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/22 03:19	https://github.…	d1c2a46a46f6	8cc079c3	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/19 16:24	https://github.…	cf8cd3cd03e2	49f35839	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/17 11:05	https://github.…	80ecacc456c1	13761366	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/08 05:37	https://github.…	a00de5aa4da3	c9a7a4dc	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/06/29 23:50	https://github.…	123906095e30	dba0b50e	.config	log	report	syz	C		
ci-upstream-kmsan-gce	2018/07/18 09:22	https://github.…	80ecacc456c1	6d5bd5b5	.config	log	report	syz			
ci-upstream-kmsan-gce	2021/06/25 14:01	https://github.…	a520ce29b172	0edbbe31	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 15:05	https://github.…	ee9407ea37bf	f9e341e3	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 14:04	https://github.…	ee9407ea37bf	f9e341e3	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 12:09	https://github.…	ee9407ea37bf	f9e341e3	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 06:44	https://github.…	ee9407ea37bf	d2d6e680	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 05:13	https://github.…	ee9407ea37bf	d2d6e680	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 02:44	https://github.…	ee9407ea37bf	d2d6e680	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/06 01:41	https://github.…	ee9407ea37bf	d2d6e680	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/05 17:22	https://github.…	925ba2a2a2fd	7f7bb950	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/05 00:14	https://github.…	b87ff0bc1209	b97d64c9	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/04 20:31	https://github.…	b87ff0bc1209	b97d64c9	.config	log	report			info	KMSAN:

Manager	Time	Kernel	Commit	Syzkaller	Config	Log	Report	Syz repro	C repro	VM info	
ci-upstream-kmsan-gce-386	2021/08/04 19:15	https://github....	b87ff0bc1209	b97d64c9	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/04 04:31	https://github....	fc388325c43b	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/03 22:59	https://github....	fc388325c43b	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/03 15:29	https://github....	fc388325c43b	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/03 14:59	https://github....	fc388325c43b	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/03 09:49	https://github....	d41122e877c7	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/03 03:44	https://github....	d41122e877c7	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/01 19:21	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/01 15:57	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/01 08:59	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/08/01 05:50	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/31 23:47	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/31 11:30	https://github....	dfab4dc3af38	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/31 04:48	https://github....	a2a37c61659d	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/31 02:14	https://github....	a2a37c61659d	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/31 01:02	https://github....	a2a37c61659d	6c236867	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/30 05:47	https://github....	e89364d49ff0	c585c7b0	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/30 04:37	https://github....	e89364d49ff0	c585c7b0	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/30 03:23	https://github....	e89364d49ff0	c585c7b0	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 21:26	https://github....	e89364d49ff0	b44001ce	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 19:56	https://github....	e89364d49ff0	b44001ce	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 15:48	https://github....	981c4ec7b5ad	b44001ce	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 12:15	https://github....	981c4ec7b5ad	b44001ce	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 08:06	https://github....	981c4ec7b5ad	9a4781d4	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 06:40	https://github....	981c4ec7b5ad	9a4781d4	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/29 02:49	https://github....	981c4ec7b5ad	9a4781d4	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/28 23:36	https://github....	981c4ec7b5ad	9a4781d4	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/28 10:05	https://github....	981c4ec7b5ad	17d6ab15	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/28 05:33	https://github....	981c4ec7b5ad	17d6ab15	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/27 23:47	https://github....	981c4ec7b5ad	17d6ab15	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/27 22:17	https://github....	981c4ec7b5ad	17d6ab15	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/27 17:53	https://github....	e8a3c6c03fa1	fd511809	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/27 04:29	https://github....	e8a3c6c03fa1	fd511809	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/27 02:24	https://github....	e8a3c6c03fa1	fd511809	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/26 17:02	https://github....	e8a3c6c03fa1	fd511809	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/07/26 12:00	https://github....	a43e029dee89	fd511809	.config	log	report			info	KMSAN:
ci-upstream-kmsan-gce-386	2021/01/07 08:36	https://github....	73d62e81b476	c104d4a3	.config	log	report			info	

* ~~*Struck through*~~ *repros no longer work on HEAD.*