KASAN: use-after-free Read in cipso_v4_genopt

Status: fixed on 2021/11/10 02:36
Reported-by: syzbot+9ec037722d2603a9f52e@syzkaller.appspotmail.com
Fix commit: ad5d07f4a9cd cipso,calipso: resolve a number of problems with the DOI refcounts 1165affd4848 net: mac802154: Fix general protection fault
First crash: 658d, last: 653d

Cause bisection: the issue happens on the oldest tested release (bisect log)
Crash: KASAN: use-after-free Read in cipso_v4_genopt (log)
Repro: C syz .config

duplicates (1):

Title	Repro	Cause bisect	Fix bisect	Count	Last	Reported	Patched	Status
KASAN: use-after-free Write in cipso_v4_doi_putdef				2	654d	653d	0/24	closed as dup on 2021/03/05 07:49

Patch testing requests:

Created	Duration	User	Patch	Repo	Result
2021/03/04 11:31	13m	paskripkin@gmail.com		https://linux.g…	report log

Sample crash report:

```
==================================================================
BUG: KASAN: use-after-free in cipso_v4_genopt+0x1078/0x1700 net/ipv4/cipso_ipv4.c:1784
Read of size 1 at addr ffff8881437d5710 by task syz-executor557/8392

CPU: 1 PID: 8392 Comm: syz-executor557 Not tainted 5.12.0-rc1-syzkaller #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011
Call Trace:
 __dump_stack lib/dump_stack.c:79 [inline]
 dump_stack+0x125/0x19e lib/dump_stack.c:120
 print_address_description+0x5f/0x3a0 mm/kasan/report.c:232
 __kasan_report mm/kasan/report.c:399 [inline]
 kasan_report+0x15e/0x210 mm/kasan/report.c:416
 cipso_v4_genopt+0x1078/0x1700 net/ipv4/cipso_ipv4.c:1784
 cipso_v4_sock_setattr+0x7c/0x460 net/ipv4/cipso_ipv4.c:1866
 netlbl_sock_setattr+0x28e/0x2f0 net/netlabel/netlabel_kapi.c:995
 smack_netlbl_add security/smack/smack_lsm.c:2404 [inline]
 smack_socket_post_create+0x13b/0x280 security/smack/smack_lsm.c:2774
 security_socket_post_create+0x6f/0xd0 security/security.c:2122
 __sock_create+0x62f/0x8c0 net/socket.c:1424
 sock_create net/socket.c:1459 [inline]
 __sys_socket+0xde/0x2d0 net/socket.c:1501
 __do_sys_socket net/socket.c:1510 [inline]
 __se_sys_socket net/socket.c:1508 [inline]
 __x64_sys_socket+0x76/0x80 net/socket.c:1508
```

Crashes (5):

Manager	Time	Kernel	Commit	Syzkaller	Config	Log	Report	Syz repro	C repro	VM info	Title
ci-upstream-kasan-gce-smack-root	2021/03/02 19:24	upstream	7a7fd0de4a98	92ead296	.config	log	report	syz	C		KASAN: use-after-free Read in cipso_v4_genopt
ci-upstream-kasan-gce-smack-root	2021/03/03 19:25	upstream	f69d02e37a85	06ed56cd	.config	log	report			info	KASAN: use-after-free Read in cipso_v4_genopt
ci-upstream-kasan-gce-smack-root	2021/03/02 14:30	upstream	7a7fd0de4a98	92ead296	.config	log	report			info	KASAN: use-after-free Read in cipso_v4_genopt
ci-upstream-kasan-gce-smack-root	2021/02/27 22:34	upstream	5695e5161974	4c37c133	.config	log	report			info	KASAN: use-after-free Read in cipso_v4_genopt
ci-upstream-kasan-gce-smack-root	2021/02/26 10:56	upstream	2c87f7a38f93	76f7fc95	.config	log	report			info	KASAN: use-after-free Read in cipso_v4_genopt

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