strongSwan - Issue #3452

*** buffer overflow detected ***:

21.05.2020 09:28 - liuuwqia liuuwqia

Status:	Rejected		
Priority:	Normal		
Assignee:			
Category:			
Affected version:	5.8.4	**Resolution:**	Invalid

Description

When I updated the strongswan from 5.7.2 to 5.8.4, I encountered a problem with the * **buffer overflow detected** * while conducting ipsec negotiations. I don't know why this happened. Here is my GDB information:
17[IKE] maximum IKE_SA lifetime 15017s
17[CFG] selected proposal: ESP:AES_CBC_128/HMAC_SHA2_256_128/NO_EXT_SEQ

- buffer overflow detected ***: /usr/local/libexec/ipsec/charon terminated

Thread 18 "charon" received signal SIGABRT, Aborted.
[Switching to Thread 0x7fffd0ff1700 (LWP 3017)]
GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51 ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0 _GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1 *0x00007ffff7303801 in __GI_abort () at abort.c:79*
#2 *0x00007ffff734c897 in __libc_message (action=action@entry=(do_abort | do_backtrace), fmt=fmt@entry=0x7ffff7479988 "*** %s ***: %s terminated\n") at ../sysdeps/posix/libc_fatal.c:181*
#3 *0x00007ffff73f7cff in __GI_*fortify_fail_abort (need_backtrace=need_backtrace@entry=true, msg=msg@entry=0x7ffff7479905 "buffer overflow detected") at fortify_fail.c:33
#4 0x00007ffff73f7d21 in *GI_*fortify_fail (msg=msg@entry=0x7ffff7479905 "buffer overflow detected") at fortify_fail.c:44
#5 0x00007ffff73f5a10 in *GI_*chk_fail () at chk_fail.c:28
#6 0x00007ffff73f4e49 in __strncpy_chk (s1=s1@entry=0x1300ae36b "", s2=s2@entry=0x7fffa00037c0 "GigabitEthernetb/0/0", n=<optimized out>, s1len=s1len@entry=0) at strncpy_chk.c:26
#7 0x00007ffff6910e54 in strncpy (_len=<optimized out>, __src=0x7fffa00037c0 "GigabitEthernetb/0/0", __dest=<optimized out>) at /usr/include/x86_64-linux-gnu/bits/string_fortified.h:106
#8 get_sw_if_index (interface=0x7fffa00037c0 "GigabitEthernetb/0/0") at kernel_vpp_ipsec.c:369
#9 manage_policy (this=0x5555557713b0, add=<optimized out>, id=0x7fffd0ff0a20, data=<optimized out>) at kernel_vpp_ipsec.c:678
#10 0x00007ffff7902544 in install_policies_inbound (type=POLICY_IPSEC, other_sa=0x7fffd0ff0b10, manual_prio=0, priority=POLICY_PRIORITY_DEFAULT, my_sa=0x23bc39ca00000000, other_ts=<optimized out>, my_ts=<optimized out>, other_addr=<optimized out>, my_addr=<optimized out>, this=0x7fffb0000e10) at sa/child_sa.c:1024
#11 install_policies_internal (this=this@entry=0x7fffb0000e10, my_addr=0x7fffb00048c0, other_addr=0x7fffb00049b0, my_ts=0x7fffa0000cc0, other_ts=0x7fffa0002e60, my_sa=my_sa@entry=0x7fffd0ff0af0, other_sa=0x7fffd0ff0b10, priority=POLICY_PRIORITY_DEFAULT, manual_prio=0, outbound=true, type=POLICY_IPSEC) at sa/child_sa.c:1097
#12 0x00007ffff7902744 in install_policies (this=0x7fffb0000e10) at sa/child_sa.c:1289
#13 0x00007ffff791bf1d in select_and_install (this=this@entry=0x7fff9c0021d0, no_dh=no_dh@entry=true, ike_auth=ike_auth@entry=true) at sa/ikev2/tasks/child_create.c:790
#14 0x00007ffff791d4e8 in process_i (this=0x7fff9c0021d0, message=0x7fffc0001740) at sa/ikev2/tasks/child_create.c:1760
#15 0x00007ffff7915f59 in process_response (message=0x7fffc0001740, this=0x7fff9c0019f0) at sa/ikev2/task_manager_v2.c:762
#16 process_message (this=0x7fff9c0019f0, msg=0x7fffc0001740) at sa/ikev2/task_manager_v2.c:1721
#17 0x00007ffff7904c27 in process_message (this=0x7fff9c001200, message=0x7fffc0001740) at sa/ike_sa.c:1586
#18 0x00007ffff78fe50f in execute (this=0x7fffc0001a90) at processing/jobs/process_message_job.c:74
#19 0x00007ffff7b9fe66 in process_job (worker=0x5555557a1f10, this=0x55555575aa70) at processing/processor.c:235
#20 process_jobs (worker=0x5555557a1f10) at processing/processor.c:321
#21 0x00007ffff7bb23db in thread_main (this=0x5555557a1f40) at threading/thread.c:331
#22 0x00007ffff76bb6db in start_thread (arg=0x7fffd0ff1700) at pthread_create.c:463
#23 0x00007ffff73e488f in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:95

I hope someone can help me,thankyou

History

#1 - 21.05.2020 09:45 - Noel Kuntze

- Status changed from New to Rejected

- Resolution set to Invalid

```
Thread 18 "charon" received signal SIGABRT, Aborted.
[Switching to Thread 0x7fffd0ff1700 (LWP 3017)]
GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
51 ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0 _GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:51
#1 0x00007ffff7303801 in __GI_abort () at abort.c:79
#2 0x00007ffff734c897 in __libc_message (action=action@entry=(do_abort | do_backtrace), fmt=fmt@entry=0x7ffff7
479988 "*** %s ***: %s terminated\n") at ../sysdeps/posix/libc_fatal.c:181
#3 0x00007ffff73f7cff in __GI_fortify_fail_abort (need_backtrace=need_backtrace@entry=true, msg=msg@entry=0x7f
fff7479905 "buffer overflow detected") at fortify_fail.c:33
#4 0x00007ffff73f7d21 in GI_fortify_fail (msg=msg@entry=0x7ffff7479905 "buffer overflow detected") at fortify_
fail.c:44
#5 0x00007ffff73f5a10 in GI_chk_fail () at chk_fail.c:28
#6 0x00007ffff73f4e49 in __strncpy_chk (s1=s1@entry=0x1300ae36b "", s2=s2@entry=0x7fffa00037c0 "GigabitEtherne
tb/0/0", n=<optimized out>, s1len=s1len@entry=0) at strncpy_chk.c:26
#7 0x00007ffff6910e54 in strncpy (_len=<optimized out>, __src=0x7fffa00037c0 "GigabitEthernetb/0/0", __dest=<o
ptimized out>) at /usr/include/x86_64-linux-gnu/bits/string_fortified.h:106
#8 get_sw_if_index (interface=0x7fffa00037c0 "GigabitEthernetb/0/0") at kernel_vpp_ipsec.c:369
#9 manage_policy (this=0x5555557713b0, add=<optimized out>, id=0x7fffd0ff0a20, data=<optimized out>) at kernel
_vpp_ipsec.c:678
[...]
```

The issue is clearly caused by custom code that was introduced by you. Therefore the issue is rejected.
So fix it yourself. We don't have that code here and henceforth can't possibly help, beyond clearly that the length argument to strncpy indicates that the buffer is longer than it actually is.