strongSwan - Bug #216

strongswan 4.6.4 (and previous) charon crashes repeatinly on x86 CentOS 5.8

13.08.2012 11:45 - Johannes Walch

Status:	Closed	**Start date:**	13.08.2012
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.0.1		
Affected version:	4.6.4	**Resolution:**	Fixed

Description

I have built strongswan 4.6.4 (and 4.6.3 for testing) on CentOS 5.8 i386. For testing I use an ipsec.conf file with 460 conn entries. charon keeps crashing with "charon: 15[DMN] killing ourself, received critical signal" messages. If I reduced the number of connections to 100 this does not happen (exact treshold not yet found).

The environment is a VM (tried with XEN and Parallels) with 1 or 2 cores and up to 1GB of RAM, always same symptoms.

Here is a backtrace from gdb

```
Core was generated by `/usr/libexec/strongswan/charon --use-syslog'.
Program terminated with signal 6, Aborted.
#0  0x00766402 in __kernel_vsyscall ()
(gdb) backtrace
#0  0x00766402 in __kernel_vsyscall ()
#1  0x00dafdf0 in raise () from /lib/libc.so.6
#2  0x00db1701 in abort () from /lib/libc.so.6
#3  0x08048fcc in segv_handler ()
#4  <signal handler called>
#5  0x00df7007 in memset () from /lib/libc.so.6
#6  0x00308744 in calc_range (this=0x8c23cd0, netbits=<value optimized out>) at selectors/traffic_selector.c:121
#7  0x003088b3 in traffic_selector_create_from_subnet (net=0x8c23c18, netbits=255 '\377', protocol=0 '\000', port=0)
    at selectors/traffic_selector.c:780
#8  0x003efbf4 in add_ts (this=<value optimized out>, end=0xb430114c, child_cfg=0x8c239c8, local=true)
    at stroke_config.c:778
#9  0x003f04ee in build_child_cfg (this=0x8b65c40, msg=0xb4301090) at stroke_config.c:851
#10 add (this=0x8b65c40, msg=0xb4301090) at stroke_config.c:898
#11 0x003ee2dc in stroke_add_conn (ctx=0x8c22af8) at stroke_socket.c:241
#12 process (ctx=0x8c22af8) at stroke_socket.c:629
#13 0x00307285 in execute (this=0x8c22b28) at processing/jobs/callback_job.c:204
#14 0x00307a17 in process_jobs (this=0x8b43088) at processing/processor.c:188
#15 0x00309f1d in thread_main (this=0x8b679d8) at threading/thread.c:305
#16 0x00861852 in start_thread () from /lib/libpthread.so.0
#17 0x00e581fe in clone () from /lib/libc.so.6
```

In 5.0.0 charon handles this config file fine (no crashes), however I am not sure about production quality of IKEv1 in 5.0.0
Would you advise upgrading to 5.0.0?

Associated revisions

Revision 305d98b7 - 13.08.2012 13:46 - Tobias Brunner

Validate netmask in traffic_selector_create_from_subnet

Fixes #216.

History

#1 - 13.08.2012 11:52 - Johannes Walch

Of course I am available to provide any additional information that could be helpful.

Kernel is 2.6.18-308.11.1.el5 from CentOS Base repo.

#2 - 13.08.2012 12:10 - Johannes Walch

The exact limit of conn sections is 208. Anything above that will result in described behaviour.
At 208 there is still plenty of free memory and no OOM errors can be seen.

#3 - 13.08.2012 13:02 - Tobias Brunner

- File 0001-Validate-netmask-in-traffic_selector_create_from_sub.patch added

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

The interesting bit is this:

> netbits=255

For unknown reasons there is no code to validate this value (neither in stroke_config.c nor in traffic_selector.c). So this is certainly a bug (please try the attached patch for a fix), but one that is not explicitly fixed with 5.0.0. Therefore, the question is where does this value come from. Do you have a netmask larger than 32 (IPv4) or 128 (IPv6) configured in ipsec.conf? Or perhaps a negative number? Could you post the ipsec.conf file that causes this problem, perhaps we can reproduce it here.

#4 - 13.08.2012 13:06 - Johannes Walch

I had two connections with /255.255.255.248 style network masks. Removing those solved the problem.

#5 - 13.08.2012 13:07 - Johannes Walch

explicitely

```
rightsubnet=172.16.16.33/255.255.255.255
leftsubnet=192.168.169.40/255.255.255.248

rightsubnet=172.16.16.34/255.255.255.255
leftsubnet=192.168.169.40/255.255.255.248
```

#6 - 13.08.2012 13:57 - Tobias Brunner

- Status changed from Feedback to Resolved

- Target version set to 5.0.1

- Resolution set to Fixed

Yep, the netmask has to be defined in CIDR notation. The parser simply reads the first number after the / and uses that as netmask.

I still pushed the patch to master as it at least fixes the crash even though the config does not result in what the user probably expects.

#7 - 13.08.2012 14:03 - Johannes Walch

Tobias Brunner wrote:

> Yep, the netmask has to be defined in CIDR notation. The parser simply reads the first number after the / and uses that as netmask.
>
> I still pushed the patch to master as it at least fixes the crash even though the config does not result in what the user probably expects.

I would humbly suggest a simple parser for the netmask, i.e check for a number betwenn 0 and 32 :)

#8 - 06.09.2012 15:38 - Tobias Brunner

- Status changed from Resolved to Closed

Files

0001-Validate-netmask-in-traffic_selector_create_from_sub.patch	893 Bytes	13.08.2012	Tobias Brunner