strongSwan - Bug #452

Run "ipsec pki" on Debian VPS got "Segmentation fault" error

21.11.2013 07:32 - Haifeng Wang

Status:	Closed	**Start date:**	21.11.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	pki		
Target version:	5.1.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

I replicated this issue on local Debian and a KVM VPS from hostigation.com.
Issue: After compiled and install Strongswan on the Debian, and run "ipsec pki" or "pki" command, returns "Segmentation fault" error, and command failed to execute.
Environment:
Debian 6 and Debian 7

```
root@debian:~# uname -a
Linux debian 2.6.32-5-amd64 #1 SMP Sun Sep 23 10:07:46 UTC 2012 x86_64 GNU/Linux
root@debian:~# more /etc/debian_version
6.0.6

root@s01:~# uname -a
Linux s01 3.2.0-4-686-pae #1 SMP Debian 3.2.46-1 i686 GNU/Linux
root@s01:~# more /etc/debian_version
7.1
```

Configuration for compile:

```
./configure  --enable-eap-identity --enable-eap-md5 \
--enable-eap-mschapv2  --enable-eap-tls   --enable-eap-ttls    --enable-eap-peap  \
--enable-eap-tnc    --enable-eap-dynamic  --enable-eap-radius   --enable-xauth-eap  \
--enable-xauth-pam    --enable-dhcp    --enable-openssl  --enable-addrblock --enable-unity  \
--enable-certexpire --enable-radattr --enable-tools --enable-openssl --disable-gmp
```

Strongswan version 5.1.1

Related issues:

Has duplicate Bug #465: It is a bug?	**Rejected**	**13.12.2013**

Associated revisions

Revision 079e6c2b - 23.01.2014 10:12 - Tobias Brunner

pki: Increase MAX_COMMANDS to cover all currently available commands

Fixes #452.

History

#1 - 21.11.2013 07:33 - Haifeng Wang

Issue:

```
root@debian:~# which ipsec
/usr/local/sbin/ipsec
root@debian:~# ipsec pki
Segmentation fault
```

#2 - 21.11.2013 10:41 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

Could you please provide a backtrace either of running *pki* in gdb or from a core dump.

#3 - 21.11.2013 10:52 - Haifeng Wang

```
(gdb) run
Starting program: /usr/local/bin/pki
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/i686/cmov/libthread_db.so.1".
strongSwan 5.1.1 PKI tool

Program received signal SIGSEGV, Segmentation fault.
0x0804b1c9 in command_usage (error=0x0) at command.c:182
182                     fprintf(out, "loaded plugins: %s\n",
```

#4 - 21.11.2013 12:33 - Tobias Brunner

I can't reproduce this. A segmentation fault at that point is also quite strange because it follows seemingly successful calls to both fprintf() and methods of lib->plugins.

Did you by any chance install your self-compiled version over Debian's default strongswan package? If so, perhaps the wrong libstrongswan shared library is used, the one installed in /usr/lib by the package and not yours in /usr/local/lib/ipsec. The loaded_plugins() method, which is called on the line where the program segfaulted, was added with 4.6.2 and Debian still ships older versions. If this is the case try uninstalling the old version (calling ldconfig might help too).

#5 - 26.11.2013 04:28 - Haifeng Wang

I uninstalled and recompiled strongswan with following configuration

```
./configure  --prefix=/usr --sysconfdir=/etc --libexecdir=/usr/lib --with-ipsecdir=/usr/lib/ipsec \
--enable-eap-identity --enable-eap-md5 \
--enable-eap-mschapv2  --enable-eap-tls   --enable-eap-ttls    --enable-eap-peap  \
--enable-eap-tnc    --enable-eap-dynamic  --enable-eap-radius   --enable-xauth-eap  \
--enable-xauth-pam    --enable-dhcp    --enable-openssl  --enable-addrblock --enable-unity  \
--enable-certexpire --enable-radattr --enable-tools --enable-openssl --disable-gmp
```

Also updated ld.so.conf for library

```
root@s01:/tmp/strongswan-5.1.1/src/pki# ldconfig -p|grep strongswan
        libstrongswan.so.0 (libc6) => /usr/lib/ipsec/libstrongswan.so.0
        libstrongswan.so (libc6) => /usr/lib/ipsec/libstrongswan.so
```

But the issue not resolved.

```
(gdb) n
182                     fprintf(out, "loaded plugins: %s\n",
3: lib->plugins->loaded_plugins(lib->plugins) = <error: Cannot access memory at address 0x1c>
2: lib->plugins = (plugin_loader_t *) 0x0
1: lib = (library_t *) 0x8057008
(gdb) n

Program received signal SIGSEGV, Segmentation fault.
0x0804b1b9 in command_usage (error=0x0) at command.c:182
182                     fprintf(out, "loaded plugins: %s\n",
3: lib->plugins->loaded_plugins(lib->plugins) = <error: Cannot access memory at address 0x1c>
2: lib->plugins = (plugin_loader_t *) 0x0
1: lib = (library_t *) 0x8057008
(gdb) n

Program terminated with signal SIGSEGV, Segmentation fault.
```

There is a Linode VPS I installed successfully, but other VPS keep failed for the "pki" command.

#6 - 26.11.2013 10:23 - Tobias Brunner

Could you post the output of ldd /usr/bin/pki?

#7 - 27.11.2013 02:41 - Haifeng Wang

```
root@s01:~# ldd /usr/bin/pki
        linux-gate.so.1 =>  (0xb774f000)
```

```
        libstrongswan.so.0 => /usr/lib/ipsec/libstrongswan.so.0 (0xb76fe000)
        libc.so.6 => /lib/i386-linux-gnu/i686/cmov/libc.so.6 (0xb759b000)
        libpthread.so.0 => /lib/i386-linux-gnu/i686/cmov/libpthread.so.0 (0xb7581000)
        libdl.so.2 => /lib/i386-linux-gnu/i686/cmov/libdl.so.2 (0xb757d000)
        librt.so.1 => /lib/i386-linux-gnu/i686/cmov/librt.so.1 (0xb7574000)
        /lib/ld-linux.so.2 (0xb7750000)
```

#8 - 27.11.2013 13:48 - Tobias Brunner

That looks ok. According to the GDB output lib->plugins is NULL. This makes no sense. If you have a look at source:src/pki/pki.c#L181 you'll see that lib->plugins->load() is called before command_usage() tries to call lib->plugins->loaded_plugins() at source:src/pki/command.c#L182. So lib->plugins should definitely be defined.

Did you patch the code somehow? Or do you load a custom plugin?

Could you try debugging this more with GDB to see why lib->plugins is suddenly NULL.

#9 - 11.12.2013 10:49 - David Maire

I have the same issue with CentOS 6.5, compiling 5.1.1 with the following options:

```
./configure --enable-xauth-noauth --sysconfdir=/etc/strongswan/ --prefix=/usr/ --localstatedir=/var/ --enable-tools --enable-openssl
```

Server itself doesn't have any problems, but the PKI tool doesn't work.

#10 - 11.12.2013 17:41 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to pki

- Status changed from Feedback to Resolved

- Target version set to 5.1.2

- Resolution set to Fixed

David Maire wrote:

> I have the same issue with CentOS 6.5, compiling 5.1.1 with the following options:

Thanks for the additional report, I was now able to reproduce this issue with CentOS 6.5 in a x64 VirtualBox VM.

The problem is that MAX_COMMANDS (since the addition of the *pkcs7* command) exactly equals the number of commands. This has the effect that the code that collects the commands and options to print the usage information does not stop at the end of the array (where it expects a NULL element) but instead iterates over the whole memory of the process (well, at least until NULL is encountered at the right position, which seems to be the case pretty early on many systems) and reassigned it, causing this segmentation fault.

I pushed a fix for this to the *pki-fixes* branch of our repository.

#11 - 12.12.2013 15:15 - David Maire

Thanks for your response. With that branch I get the following output:

```
command 'verify' registered too many options, please increase MAX_OPTIONS
command 'pkcs7' registered too many options, please increase MAX_OPTIONS
command 'signcrl' registered too many options, please increase MAX_OPTIONS
command 'print' registered too many options, please increase MAX_OPTIONS
command 'self' registered too many options, please increase MAX_OPTIONS
command 'req' registered too many options, please increase MAX_OPTIONS
command 'pub' registered too many options, please increase MAX_OPTIONS
command 'keyid' registered too many options, please increase MAX_OPTIONS
command 'issue' registered too many options, please increase MAX_OPTIONS
command 'gen' registered too many options, please increase MAX_OPTIONS
```

I don't really understand the context but I was able to 'fix' the problem by making this change in src/pki/command.c:

```
-    if (i < countof(cmds[registered].options) - 3)
+    if (countof(cmds[registered].options) - 3 > MAX_OPTIONS)
```

#12 - 12.12.2013 17:08 - Tobias Brunner

Argh, sorry about that. I thought about reversing the two branches of that if statement and evidently didn't undo enough before committing (alas without testing again). I pushed a fixed version of that commit.

#13 - 23.01.2014 10:12 - Tobias Brunner

- Status changed from Resolved to Closed

#14 - 17.02.2014 12:54 - Tobias Brunner

- Has duplicate Bug #516: some ipsec pki commands segfault added

#15 - 19.02.2014 16:12 - Tobias Brunner

- Has duplicate deleted (Bug #516: some ipsec pki commands segfault)