

strongSwan - Bug #208

[charon] SIGSEGV when compiled with O1, Os

02.08.2012 11:39 - Matija Pecotic

| | | | |
|---|--------------|------------------------|------------|
| Status: | Closed | Start date: | 02.08.2012 |
| Priority: | Normal | Due date: | |
| Assignee: | Martin Willi | Estimated time: | 0.00 hour |
| Category: | | Resolution: | |
| Target version: | 5.0.1 | | |
| Affected version: | 5.0.0 | | |
| Description | | | |
| Hello, | | | |
| recently we had SIGSEGV on charon startup when strongswan was compiled with Os or O1, while compiling with O0 produced no fault. Problem was tracked down to crypto_factory.c which got 'optimised' by compiler. Attached you can find logs of gdb session when compiled with O0 and O1 and excerpt from messages. (These could be a bit more descriptive, but I can repeat issue and obtain further info). | | | |
| Architecture is ppc, core is e500, gcc is 4.3.3 | | | |
| We use gcc 4.3.3 on our other target as well, multicore mips64, and there this issue is not occurring. | | | |
| For the mentioned target, ppc, we also use gcc 3.4.3, with it there is also no occurrence. | | | |
| Problem was originally noted with 4.5.0, reproduced with up to 5.0.0 | | | |
| We solved it in our environment by realigning the code, patch is also attached for reference. | | | |
| Do you have any comments? | | | |
| Thanks and best regards, | | | |
| Matija Pecotic | | | |

Associated revisions

Revision 11d6bc3e - 02.08.2012 12:08 - Martin Willi

Move MODP_CUSTOM va_arg fetching out of loop

It seems problematic at least on PPC with gcc 4.3, fixes #208.

History

#1 - 02.08.2012 12:12 - Martin Willi

- Status changed from New to Closed
- Assignee set to Martin Willi
- Target version set to 5.0.1

I don't have PPC here to reproduce the issue, but doing va_arg operations outside the loop shouldn't harm. I've pushed the referenced patch.

Thanks for reporting this issue.

Files

| | | | |
|-----------------------|-----------|------------|----------------|
| log_g_O0.log | 902 Bytes | 02.08.2012 | Matija Pecotic |
| log_g_o1.log | 1.5 KB | 02.08.2012 | Matija Pecotic |
| messages | 564 Bytes | 02.08.2012 | Matija Pecotic |
| code_realignent.patch | 1.2 KB | 02.08.2012 | Matija Pecotic |