strongSwan - Bug #551
NTRU tests fail with SIGSEGV
22.03.2014 19:10 - Jonathan Davies

Status: Closed
Priority: Normal
Assignee: Tobias Brunner
Category: testing
Target version: 5.1.3
Affected version: dr|rc|master
Resolution: Fixed

Description
As of today, the 12.04 daily build of strongSwan fails its NTRU tests with a SIGSEGV on amd64 only:

https://launchpadlibrarian.net/170362758/buildlog_ubuntu-precise-amd64.strongswan_5.1.2~rc2-0~10503%2B43~ubuntu12.04.1_False_TOBUILD.txt.gz

Running suite 'ntru':
  Running case 'drbg_strength': ++++++++   
  Running case 'drbg': +++   
  Running case 'drbg_reseed': +   
  Running case 'mgf1': ++   
  Running case 'trits': ++   
  Running case 'poly': ++   
  Running case 'ring_mult': ++++++++   
  Running case 'array': +++-   
  Failure in 'test_ntru_array': SIGSEGV(11) (i = 2)
    dumping 1 stack frame addresses:
      [0x2b1bf1ddf530]
  Failure in 'test_ntru_array': SIGSEGV(11) (i = 3)
    dumping 1 stack frame addresses:
      [0x2b1bf1ddf530]
  Running case 'param_set': +
  Running case 'privkey': --
  Failure in 'test_ntru_privkey': SIGSEGV(11) (i = 0)
    dumping 1 stack frame addresses:
      [0x2b1bf1dde2d0]
  Failure in 'test_ntru_privkey': SIGSEGV(11) (i = 1)
    dumping 1 stack frame addresses:
      [0x2b1bf1dde2d0]
  Running case 'ke': ++++++++   
  Running case 'retransmission': +
  Running case 'pubkey_oid': ++++++++   
  Running case 'wrong_set': +
  Running case 'ciphertext': +
  Running case 'wrong_ciphertext': +
  Passed 14/16 'ntru' test cases

I retried the build earlier and this is the second time it's happened today so it doesn't appear to be a transient issue.

Last successful build was yesterday:
https://code.launchpad.net/~strongswan/+archive/strongswan-daily/+builds?build_text=&build_state=all of commit ID b51791284873f81d31161b47db1451939456cc5.

Associated revisions
Revision 036db0a - 31.03.2014 17:00 - Tobias Brunner
unit-tests: Always load address of testable functions
The addresses can actually change as plugins are loaded/unloaded for each test case.
Fixes #551.

History

#1 - 23.03.2014 17:03 - Andreas Steffen
- Status changed from New to Feedback
- Assignee set to Andreas Steffen

Hmm, I cannot reproduce this crash on my X86_64 system. It's strange that all NTRU changes I checked in on Saturday did not concern the ntru_array test at all.

Andreas

#2 - 23.03.2014 17:06 - Jonathan Davies
Andreas Steffen wrote:

Hmm, I cannot reproduce this crash on my X86_64 system. It's strange that all NTRU changes I checked in on Saturday did not concern the ntru_array test at all.

Turns out that it was transient. Today's build went through fine:

- [https://code.launchpad.net/~strongswan/+archive/strongswan-daily/+build/5839480](https://code.launchpad.net/~strongswan/+archive/strongswan-daily/+build/5839480)

#3 - 24.03.2014 10:22 - Tobias Brunner

libstrongswan-5.1.2~rc2-0~10504+43~ubuntu12.04.1

Jonathan, why is the package version still 5.1.2~rc2? The current version is 5.1.3~dr1 ([source:configure.ac#L22](#)).

#4 - 31.03.2014 17:01 - Tobias Brunner
- Tracker changed from Issue to Bug
- Category set to testing
- Status changed from Feedback to Closed
- Assignee changed from Andreas Steffen to Tobias Brunner
- Target version set to 5.1.3
- Resolution set to Fixed

Fixed with the associated commit.