strongSwan - Bug #1156

random_rng_t::get_bytes may falsly claim to allocate random

12.10.2015 09:36 - Noam Lampert

Status:	Closed	**Start date:**	12.10.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libstrongswan		
Target version:	5.3.4		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

https://github.com/strongswan/strongswan/blob/master/src/libstrongswan/plugins/random/random_rng.c

If 'read' returns -1, then 'got' becomes -1. done will be SIZE_T_MAX (because it is unsigned). The loop will exit and return TRUE without ever allocating random.

For reference, the code:

```
METHOD(rng_t, get_bytes, bool,
    private_random_rng_t *this, size_t bytes, u_int8_t *buffer)
{
    size_t done;
    ssize_t got;

    done = 0;

    while (done < bytes)
    {
        got = read(this->fd, buffer + done, bytes - done);
        if (got <= 0)
        {
            DBG1(DBG_LIB, "reading from random FD %d failed: %s, retrying...",
                 this->fd, strerror(errno));
            sleep(1);
        }
        done += got;
    }
    return TRUE;
}
```

Associated revisions

Revision 35dbf8af - 29.10.2015 16:17 - Tobias Brunner

random: Properly handle errors when reading from /dev/[u]random

If -1 was returned on the first call to read() `done` got SIZE_MAX
and the function returned TRUE even though no actual random data had
been allocated.

Fixes #1156.

History

#1 - 12.10.2015 11:43 - Tobias Brunner

- Tracker changed from Issue to Bug

- Description updated

- Category set to libstrongswan

- Status changed from New to Feedback

- Priority changed from Urgent to Normal

- Target version set to 5.3.4

Hm, that really looks strange. Apparently it was like this since the plugin got added (6a365f0740) and the retrying was added (even worse, size_t was used for got before 4.2.8 or ceff3064fe).

I think adding a continue statement after sleep() should fix it. I pushed that to the *1156-random-read* branch.

#2 - 09.11.2015 11:20 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed