Valgrind reports uninitialized byte usage error in socket_default_socket.c

30.08.2013 21:12 - Piyush Patel

Status: Closed
Priority: Normal
Assignee: Tobias Brunner
Category: charon
Target version: 5.1.1
Affected version: 5.1.0
Resolution: Fixed

Description
Valgrind outputted the below error. This occurred while trying to setup a tunnel to the gateway. This test was doing against 5.1.0.

```
==20660== Syscall param socketcall.sendmsg(msg.msg_control) points to uninitialised byte(s)
==20660==       at 0x550A33D: ??? (syscall-template.S:82)
==20660==       by 0xA4F002C: sender (socket_default_socket.c:489)
==20660==       by 0x52A81AE: sender (socket_manager.c:87)
==20660==       by 0x52A7D3E: send_packets (sender.c:161)
==20660==       by 0x4E5B53D: execute (callback_job.c:77)
==20660==       by 0x4E5BEDF: thread_main (thread.c:309)
==20660==       by 0x5502E99: start_thread (pthread_create.c:308)
==20660==    Address 0xdd15d1c is on thread 7's stack
==20660==
```

I applied following patch and the report went away.

```
--- socket_default_socket.c.orig 2013-08-30 11:08:02.429571502 -0700
+++ socket_default_socket.c 2013-08-30 10:29:13.514055642 -0700
@@ -445,6 +445,7 @@
 #elif defined(IP_SENDSRCADDR)
     char buf[CMSG_SPACE(sizeof(struct in_addr))];
 #endif
+    memset(buf, 0, sizeof(buf));
     msg.msg_control = buf;
     msg.msg_controllen = sizeof(buf);
     cmsg = CMSG_FIRSTHDR(&msg);
```

Associated revisions
Revision 4eb6149a - 10.09.2013 13:42 - Tobias Brunner
sockets: Initialize the whole ancillary data buffer not only the actual struct

This avoids uninitialized bytes that Valgrind seems to notice otherwise.

Fixes #395.

History
#1 - 10.09.2013 14:48 - Tobias Brunner
- Tracker changed from Issue to Bug
- Description updated
- Category set to charon
- Status changed from New to Closed
- Assignee set to Tobias Brunner
- Target version set to 5.1.1
- Resolution set to Fixed

20.03.2020
Fixed with the associated commit, thanks.