libosmocore - Bug #4871

osmo_stats statsd reporter submitting broken data

11/27/2020 10:34 PM - pespin

Status:	Resolved	**Start date:**	11/27/2020
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

snprintf format being used in osmo_stats_reporter_statsd_send seems to be broken or not supported when I run libosmocore master (920491936e1d4636d55c44d2faaad4bb06de27ee) on my raspberry pi 3b+.

See how output buffer of snprintf doesn't match expected output from content of input variables:

```
Breakpoint 1, osmo_stats_reporter_statsd_send (srep=0x7400e570, name1=0x203c0 "power_meter", index
1=1,
    name2=0x1ff00 "power_meter.export_energy", value=12000, unit=0x76750ac0 "g")
    at /home/pi/dev/git/libosmocore/src/stats_statsd.c:96
96              int nchars, rc = 0;
(gdb) n
97              char *fmt = NULL;
(gdb) n
98              char *prefix = srep->name_prefix;
(gdb) n
99              int old_len = msgb_length(srep->buffer);
(gdb) n
101             if (prefix) {
(gdb) n
102                     if (name1)
(gdb)
103                             fmt = "%1$s.%2$s.%6$u.%3$s:%4$d|%5$s";
(gdb)
114             if (srep->agg_enabled) {
(gdb)
115                     if (msgb_length(srep->buffer) > 0 &&
(gdb)
122             buf = (char *)msgb_put(srep->buffer, 0);
(gdb)
123             buf_size = msgb_tailroom(srep->buffer);
(gdb)
125             nchars = snprintf(buf, buf_size, fmt,
(gdb)
129             if (nchars >= buf_size) {
(gdb) print buf
$1 = 0x71a028f4 "dosmotics.power_meter.1987381952.power_meter.export_energy:12000|(null)"
(gdb) print unit
$2 = 0x76750ac0 "g"
(gdb) print nchars
$3 = 71
(gdb) print index1
$4 = 1
(gdb) print fm
No symbol "fm" in current context.
(gdb) print fmt
$5 = 0x76750940 "%1$s.%2$s.%6$u.%3$s:%4$d|%5$s"
(gdb) info locals
buf = 0x71a028f4 "dosmotics.power_meter.1987381952.power_meter.export_energy:12000|(null)"
buf_size = 996
nchars = 71
```

```
rc = 0
fmt = 0x76750940 "%1$s.%2$s.%6$u.%3$s:%4$d|%5$s"
prefix = 0x73c693b0 "dosmotics"
old_len = 0
(gdb) print prefix
$6 = 0x73c693b0 "dosmotics"
(gdb) print name1
$7 = 0x203c0 "power_meter"
(gdb) print name2
$8 = 0x1ff00 "power_meter.export_energy"
(gdb) print value
$9 = 12000
(gdb) print unit
$10 = 0x76750ac0 "g"
(gdb) print index1
$11 = 1

Package: libc6
Version: 2.28-10+rpi1
```

Associated revisions

Revision 3f2775b4 - 11/28/2020 12:11 AM - pespin

statsd report: Fix wrong fmt specificier generating wrong stats

Fixes: OS#4871
Change-Id: I04aba0f3a4ff6563a4e285b982077184645d1180

History

#1 - 11/27/2020 11:52 PM - pespin

man snprintf:

```
 The C99 standard does not include the style using '$', which comes from the Single UNIX Specification.
...
       The glibc implementation of the functions snprintf() and vsnprintf() conforms to the C99 standard,  tha
t  is,  behaves  as  de-
       scribed above, since glibc version 2.1.  Until glibc 2.0.6, they would return -1 when the output was tr
uncated.
```

#2 - 11/28/2020 12:18 AM - pespin

- Status changed from New to Feedback

- % Done changed from 0 to 90

Fixed by:
https://gerrit.osmocom.org/c/libosmocore/+/21393 statsd report: Fix wrong fmt specificier generating wrong stats [NEW]

#3 - 11/30/2020 01:23 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100

Merged, closing.