```
**********************************************************
   80637 Sat Feb  7 18:57:40 2015
new/usr/src/lib/libdisasm/common/dis_arm.c
libdisasm: disassembly of strex may cause SIGSEGV
To make things confusing enough, the names of bitfields between ldrex and
strex are not totally consistent so this commit makes it easier on future
readers.
**********************************************************
______unchanged_portion_omitted_

1272 /*
1273  * Handle LDREX and STREX out of the extra loads/stores extensions.
1274  */
1275 static int
1276 arm_dis_lsexcl(uint32_t in, char *buf, size_t buflen)
1277 {
1278         arm_cond_code_t cc;
1279         arm_reg_t rx, ry, rz;
1279         arm_reg_t rn, rd, rm;
1280         int lbit;
1281         size_t len;

1283         /*
1284          * To make things confusing enough, the names of bitfields between
1285          * ldrex and strex are not totally consistent.  Specifically,
1286          *    STREX rd, rt, [rn]
1287          *       rn = 19:16
1288          *       rd = 15:12
1289          *       rt = 3:0
1290          *
1291          *    LDREX rt, [rn]
1292          *       rn = 19:16
1293          *       rt = 15:12
1294          *
1295          * To avoid having to do too many mental gymnastics, let's just
1296          * think of the bitfields as:
1297          *
1298          *       rx = 19:16
1299          *       ry = 15:12
1300          *       rz = 3:0
1301          *
1302          * And so we print the instructions as:
1303          *    STREX ry, rz, [rx]
1304          *    LDREX ry, [rx]
1305          */

1307 #endif /* ! codereview */
1308         cc = (in & ARM_CC_MASK) >> ARM_CC_SHIFT;
1309         rx = (in & ARM_ELS_RN_MASK) >> ARM_ELS_RN_SHIFT;
1310         ry = (in & ARM_ELS_RD_MASK) >> ARM_ELS_RD_SHIFT;
1311         rz = (in & ARM_ELS_LOW_AM_MASK);
1283         rn = (in & ARM_ELS_RN_MASK) >> ARM_ELS_RN_SHIFT;
1284         rd = (in & ARM_ELS_RD_MASK) >> ARM_ELS_RD_SHIFT;
1285         rm = in & ARM_ELS_RN_MASK;
1312         lbit = in & ARM_ELS_LBIT_MASK;

1314         len = snprintf(buf, buflen, "%s%sex %s, ",
1315             lbit != 0 ? "ldr" : "str",
1316             arm_cond_names[cc], arm_reg_names[ry]);
1290             arm_cond_names[cc], arm_reg_names[rd]);
1317         if (len >= buflen)
1318                 return (-1);

1320         if (lbit)
1321                 len += snprintf(buf + len, buflen - len, "[%s]",
1322                     arm_reg_names[rx]);
```



```
1296                     arm_reg_names[rn]);
1323         else
1324                 len += snprintf(buf + len, buflen - len, "%s, [%s]",
1325                     arm_reg_names[rz], arm_reg_names[rx]);
1299                     arm_reg_names[rm], arm_reg_names[rn]);
1326         return (len >= buflen ? -1 : 0);
1327 }
______unchanged_portion_omitted_
```