

new/usr/src/cmd/sgs/libld/common/machrel.intel.c

1

```
*****
45652 Mon Jan 21 01:45:14 2019
new/usr/src/cmd/sgs/libld/common/machrel.intel.c
10267 ld and GCC disagree about i386 local dynamic TLS
*****
_____unchanged_portion_omitted_____

418 static uchar_t tlsinstr_ld_le_movgs[] = {
418 static uchar_t tlsinstr_gd_ie_movgs[] = {
419 /*
420 * 0x00 movl %gs:0x0,%eax
420 *      movl %gs:0x0,%eax
421 */
422 0x65, 0xa1, 0x00, 0x00, 0x00, 0x00,
423 };

425 /*
426 * 0x00 nopl 0(%eax,%eax) -- the intel recommended 5-byte nop
427 * See Intel® 64 and IA-32 Architectures Software Developer's Manual
428 * Volume 2B: Instruction Set Reference, M-U
429 * Table 4-12, Recommended Multi-Byte Sequence of NOP Instruction
430 */
431 static uchar_t tlsinstr_nop5[] = {
433 0x0f, 0x1f, 0x44, 0x00, 0x00
422 0x65, 0xa1, 0x00, 0x00, 0x00, 00
434 };

436 #define TLS_GD_IE_MOV 0x8b /* movl opcode */
437 #define TLS_GD_IE_POP 0x58 /* popl + reg */

439 #define TLS_GD_LE_MOVL 0xb8 /* movl + reg */

441 #define TLS_NOP 0x90 /* NOP instruction */

443 #define MODRM_MSK_MOD 0xc0
444 #define MODRM_MSK_RO 0x38
445 #define MODRM_MSK_RM 0x07

447 #define SIB_MSK_SS 0xc0
448 #define SIB_MSK_IND 0x38
449 #define SIB_MSK_BS 0x07

451 static Fixupret
452 tls_fixups(Of1_desc *of1, Rel_desc *arsp)
453 {
454     Sym_desc      *sdp = arsp->rel_sym;
455     Word          rtype = arsp->rel_rtype;
456     uchar_t       *offset, r1, r2;

458     offset = (uchar_t *)((uintptr_t)arsp->rel_offset +
459                          (uintptr_t)elf_getxoff(arsp->rel_isdesc->is_indata) +
460                          (uintptr_t)RELAUX_GET_OSDESC(arsp->os_outdata->d_buf));

462     if (sdp->sd_ref == REF_DYN_NEED) {
463         /*
464          * IE reference model
465          */
466         switch (rtype) {
467         case R_386_TLS_GD:
468             /*
469              * Transition:
470              * 0x0 leal x@tls_gd(,r1,1), %eax
471              * 0x7 call ___tls_get_addr
472              * 0xc
473              * To:

```

new/usr/src/cmd/sgs/libld/common/machrel.intel.c

2

```

474 *      0x0 movl %gs:0, %eax
475 *      0x6 addl x@gotntpoff(r1), %eax
476 */
477 DBG_CALL(DBG_reloc_transition(of1->of1_lml, M_MACH,
478                               R_386_TLS_GOTIE, arsp, ld_reloc_sym_name));
479 arsp->rel_rtype = R_386_TLS_GOTIE;
480 arsp->rel_offset += 5;

482 /*
483 * Adjust 'offset' to beginning of instruction
484 * sequence.
485 */
486 offset -= 3;
487 r1 = (offset[2] & SIB_MSK_IND) >> 3;
488 (void) memcpy(offset, tlsinstr_gd_ie,
489              sizeof (tlsinstr_gd_ie));

491 /*
492 * set register %r1 into the addl
493 * instruction.
494 */
495 offset[0x7] |= r1;
496 return (FIX_RELOC);

498 case R_386_TLS_GD_PLT:
499     /*
500      * Fixup done via the TLS_GD relocation
501      */
502     DBG_CALL(DBG_reloc_transition(of1->of1_lml, M_MACH,
503                                   R_386_NONE, arsp, ld_reloc_sym_name));
504     return (FIX_DONE);
505 }
506 }

508 /*
509 * LE reference model
510 */
511 switch (rtype) {
512 case R_386_TLS_GD:
513     /*
514      * Transition:
515      * 0x0 leal x@tls_gd(,r1,1), %eax
516      * 0x7 call ___tls_get_addr
517      * 0xc
518      * To:
519      * 0x0 movl %gs:0, %eax
520      * 0x6 addl $x@ntpoff, %eax
521      * 0xb nop
522      * 0xc
523      */
524     DBG_CALL(DBG_reloc_transition(of1->of1_lml, M_MACH,
525                                   R_386_TLS_LE, arsp, ld_reloc_sym_name));

527     arsp->rel_rtype = R_386_TLS_LE;
528     arsp->rel_offset += 4;

530 /*
531 * Adjust 'offset' to beginning of instruction
532 * sequence.
533 */
534 offset -= 3;
535 (void) memcpy(offset, tlsinstr_gd_le,
536              sizeof (tlsinstr_gd_le));
537 return (FIX_RELOC);

539 case R_386_TLS_GD_PLT:

```

```

540     case R_386_PLT32:
541         /*
542          * Fixup done via the TLS_GD/TLS_LDM relocation processing
543          * and ld_reloc_plt() handling __tls_get_addr().
544          * Fixup done via the TLS_GD relocation
545          */
546         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
547                                     R_386_NONE, arsp, ld_reloc_sym_name));
548         return (FIX_DONE);
549
550     case R_386_TLS_LDM_PLT:
551         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
552                                     R_386_NONE, arsp, ld_reloc_sym_name));
553
554         /*
555          * Transition:
556          *   call __tls_get_addr()
557          * to:
558          *   nopl 0x0(%eax,%eax)
559          */
560         (void) memcpy(offset - 1, tlsinstr_nop5,
561                     sizeof (tlsinstr_nop5));
562         /*
563          *   nopl 0x0(%eax,%eax)
564          *   nopl 0x0(%eax,%eax)
565          *   nopl 0x0(%eax,%eax)
566          *   nopl 0x0(%eax,%eax)
567          */
568         *(offset - 1) = TLS_NOP;
569         *(offset) = TLS_NOP;
570         *(offset + 1) = TLS_NOP;
571         *(offset + 2) = TLS_NOP;
572         *(offset + 3) = TLS_NOP;
573         return (FIX_DONE);
574
575     case R_386_TLS_LDM:
576         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
577                                     R_386_NONE, arsp, ld_reloc_sym_name));
578
579         /*
580          * Transition:
581          *   0x00 leal x1@tlsldm(%ebx), %eax
582          *   0x06 call __tls_get_addr
583          * to:
584          *   0x00 movl %gs:0, %eax
585          */
586         (void) memcpy(offset - 2, tlsinstr_ld_le_movgs,
587                     sizeof (tlsinstr_ld_le_movgs));
588
589         /*
590          * We implicitly treat this as if a R_386_TLS_LDM_PLT for the
591          * __tls_get_addr call followed it as the GNU compiler
592          * doesn't generate one. This is safe, because if one __does__
593          * exist we'll just write the nop again.
594          */
595         (void) memcpy(offset + 4, tlsinstr_nop5,
596                     sizeof (tlsinstr_nop5));
597         (void) memcpy(offset - 2, tlsinstr_gd_ie_movgs,
598                     sizeof (tlsinstr_gd_ie_movgs));
599         return (FIX_DONE);
600
601     case R_386_TLS_LD0_32:
602         /*

```

```

603         * Instructions:
604         *   0x10 leal x1@dtppoff(%eax), %edx      R_386_TLS_LD0_32
605         *   to
606         *   0x10 leal x1@ntppoff(%eax), %edx      R_386_TLS_LE
607         */
608         offset -= 2;
609
610         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
611                                     R_386_TLS_LE, arsp, ld_reloc_sym_name));
612         arsp->rel_rtype = R_386_TLS_LE;
613         return (FIX_RELOC);
614
615     case R_386_TLS_GOTIE:
616         /*
617          * These transitions are a little different than the
618          * others, in that we could have multiple instructions
619          * pointed to by a single relocation. Depending upon the
620          * instruction, we perform a different code transition.
621          *
622          * Here's the known transitions:
623          *
624          * 1) movl foo@gotntppoff(%reg1), %reg2
625          *   0x8b, 0x80 | (reg2 << 3) | reg1, foo@gotntppoff
626          *
627          * 2) addl foo@gotntppoff(%reg1), %reg2
628          *   0x03, 0x80 | (reg2 << 3) | reg1, foo@gotntppoff
629          *
630          * Transitions IE -> LE
631          *
632          * 1) movl $foo@ntppoff, %reg2
633          *   0xc7, 0xc0 | reg2, foo@ntppoff
634          *
635          * 2) addl $foo@ntppoff, %reg2
636          *   0x81, 0xc0 | reg2, foo@ntppoff
637          *
638          * Note: reg1 != 4 (%esp)
639          */
640         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
641                                     R_386_TLS_LE, arsp, ld_reloc_sym_name));
642         arsp->rel_rtype = R_386_TLS_LE;
643
644         offset -= 2;
645         r2 = (offset[1] & MODRM_MSK_R0) >> 3;
646         if (offset[0] == 0x8b) {
647             /* case 1 above */
648             offset[0] = 0xc7; /* movl */
649             offset[1] = 0xc0 | r2;
650             return (FIX_RELOC);
651         }
652
653         if (offset[0] == 0x03) {
654             /* case 2 above */
655             assert(offset[0] == 0x03);
656             offset[0] = 0x81; /* addl */
657             offset[1] = 0xc0 | r2;
658             return (FIX_RELOC);
659         }
660
661         /*
662          * Unexpected instruction sequence - fatal error.
663          */
664         {
665             Conv_inv_buf_t inv_buf;

```

```

658         ld_eprintf(of1, ERR_FATAL, MSG_INTL(MSG_REL_BADTLSINS),
659                    conv_reloc_386_type(arsp->rel_rtype, 0, &inv_buf),
660                    arsp->rel_isdesc->is_file->ifl_name,
661                    ld_reloc_sym_name(arsp),
662                    arsp->rel_isdesc->is_name,
663                    EC_OFF(arsp->rel_roffset));
664     }
665     return (FIX_ERROR);

667 case R_386_TLS_IE:
668     /*
669     * These transitions are a little different than the
670     * others, in that we could have multiple instructions
671     * pointed to by a single relocation. Depending upon the
672     * instruction, we perform a different code transition.
673     *
674     * Here's the known transitions:
675     * 1) movl foo@indntpoff, %eax
676     *    0xa1, foo@indntpoff
677     *
678     * 2) movl foo@indntpoff, %eax
679     *    0x8b, 0x05 | (reg << 3), foo@gotntpoff
680     *
681     * 3) addl foo@indntpoff, %eax
682     *    0x03, 0x05 | (reg << 3), foo@gotntpoff
683     *
684     * Transitions IE -> LE
685     *
686     * 1) movl $foo@ntpoff, %eax
687     *    0xb8, foo@ntpoff
688     *
689     * 2) movl $foo@ntpoff, %reg
690     *    0xc7, 0xc0 | reg, foo@ntpoff
691     *
692     * 3) addl $foo@ntpoff, %reg
693     *    0x81, 0xc0 | reg, foo@ntpoff
694     */
695     arsp->rel_rtype = R_386_TLS_LE;
696     offset--;
697     if (offset[0] == 0xa1) {
698         /* case 1 above */
699         offset[0] = 0xb8;      /* movl */
700         return (FIX_RELOC);
701     }

703     offset--;
704     if (offset[0] == 0x8b) {
705         /* case 2 above */
706         r2 = (offset[1] & MODRM_MSK_R0) >> 3;
707         offset[0] = 0xc7;      /* movl */
708         offset[1] = 0xc0 | r2;
709         return (FIX_RELOC);
710     }
711     if (offset[0] == 0x03) {
712         /* case 3 above */
713         r2 = (offset[1] & MODRM_MSK_R0) >> 3;
714         offset[0] = 0x81;      /* addl */
715         offset[1] = 0xc0 | r2;
716         return (FIX_RELOC);
717     }
718     /*
719     * Unexpected instruction sequence - fatal error.
720     */
721     {
722         Conv_inv_buf_t inv_buf;

```

```

724         ld_eprintf(of1, ERR_FATAL, MSG_INTL(MSG_REL_BADTLSINS),
725                    conv_reloc_386_type(arsp->rel_rtype, 0, &inv_buf),
726                    arsp->rel_isdesc->is_file->ifl_name,
727                    ld_reloc_sym_name(arsp),
728                    arsp->rel_isdesc->is_name,
729                    EC_OFF(arsp->rel_roffset));
730     }
731     return (FIX_ERROR);
732 }
733 return (FIX_RELOC);
734 }

```

unchanged portion omitted

88680 Mon Jan 21 01:45:14 2019

new/usr/src/cmd/sgs/packages/common/SUNWworld-README
10267 ld and GCC disagree about i386 local dynamic TLS

```

1 #
2 # Copyright (c) 1996, 2010, Oracle and/or its affiliates. All rights reserved.
3 #
4 # CDDL HEADER START
5 #
6 # The contents of this file are subject to the terms of the
7 # Common Development and Distribution License (the "License").
8 # You may not use this file except in compliance with the License.
9 #
10 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
11 # or http://www.opensolaris.org/os/licensing.
12 # See the License for the specific language governing permissions
13 # and limitations under the License.
14 #
15 # When distributing Covered Code, include this CDDL HEADER in each
16 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
17 # If applicable, add the following below this CDDL HEADER, with the
18 # fields enclosed by brackets "[]" replaced with your own identifying
19 # information: Portions Copyright [yyyy] [name of copyright owner]
20 #
21 # CDDL HEADER END
22 #
23 # Note: The contents of this file are used to determine the versioning
24 # information for the SGS toolset. The number of CRS listed in
25 # this file must grow monotonically, or the SGS version will
26 # move backwards, causing a great deal of confusion. As such,
27 # CRS must never be removed from this file. See
28 # libconv/common/bld_vernote.ksh, and bug#4519569 for more
29 # details on SGS versioning.
30 #
31 -----
32 SUNWworld - link-editors development package.
33 -----
34
35 The SUNWworld package is an internal development package containing the
36 link-editors and some related tools. All components live in the OSNET
37 source base, but not all components are delivered as part of the normal
38 OSNET consolidation. The intent of this package is to provide access
39 to new features/bugfixes before they become generally available.
40
41 General link-editor information can be found:
42
43     http://linkers.central/
44     http://linkers.sfbay/      (also known as linkers.eng)
45
46 Comments and Questions:
47
48     Contact Rod Evans, Ali Bahrami, and/or Seizo Sakurai.
49
50 Warnings:
51
52     The postremove script for this package employs /usr/sbin/static/mv,
53     and thus, besides the common core dependencies, this package also
54     has a dependency on the SUNWsutl package.
55
56 Patches:
57
58     If the patch has been made official, you'll find it in:
59
60     http://sunsolve.east/cgi/show.pl?target=patches/os-patches

```

```

62     If it hasn't been released, the patch will be in:
63
64     /net/sunsoftpatch/patches/temporary
65
66 Note, any patches logged here refer to the temporary ("T") name, as we
67 never know when they're made official, and although we try to keep all
68 patch information up-to-date the real status of any patch can be
69 determined from:
70
71     http://sunsoftpatch.eng
72
73     If it has been obsoleted, the patch will be in:
74
75     /net/on${RELEASE}-patch/on${RELEASE}/patches/${MACH}/obsolete
76
77 History:
78
79 Note, starting after Solaris 10, letter codes in parenthesis may
80 be found following the bug synopsis. Their meanings are as follows:
81
82     (D) A documentation change accompanies the implementation change.
83     (P) A packaging change accompanies the implementation change.
84
85 In all cases, see the implementation bug report for details.
86
87 The following bug fixes exist in the OSNET consolidation workspace
88 from which this package is created:
89
90 -----
91 Solaris 8
92 -----
93 Bugid    Risk Synopsis
94 =====
95 4225937 i386 linker emits sparc specific warning messages
96 4215164 shf_order flag handling broken by fix for 4194028.
97 4215587 using ld and the -r option on solaris 7 with compiler option -xarch=v9
98         causes link errors.
99 4234657 103627-08 breaks purify 4.2 (plt padding should not be enabled for
100         32-bit)
101 4235241 dbx no longer gets dlclose notification.
102 -----
103 All the above changes are incorporated in the following patches:
104 Solaris/SunOS 5.7_sparc      patch 106950-05 (never released)
105 Solaris/SunOS 5.7_x86       patch 106951-05 (never released)
106 Solaris/SunOS 5.6_sparc     patch 107733-02 (never released)
107 Solaris/SunOS 5.6_x86       patch 107734-02
108 -----
109 4248290 inetd dumps core upon bootup - failure in dlclose() logic.
110 4238071 dlopen() leaks while descriptors under low memory conditions
111 -----
112 All the above changes are incorporated in the following patches:
113 Solaris/SunOS 5.7_sparc     patch 106950-06
114 Solaris/SunOS 5.7_x86       patch 106951-06
115 Solaris/SunOS 5.6_sparc     patch 107733-03 (never released)
116 Solaris/SunOS 5.6_x86       patch 107734-03
117 -----
118 4267980 INITFIRST flag of the shard object could be ignored.
119 -----
120 All the above changes plus:
121 4238973 fix for 4121152 affects linking of Ada objects
122 4158744 patch 103627-02 causes core when RPATH has blank entry and
123         dlopen/dlclose is used
124 are incorporated in the following patches:
125 Solaris/SunOS 5.5.1_sparc   patch 103627-12 (never released)
126 Solaris/SunOS 5.5.1_x86     patch 103628-11

```

```

128 -----
129 4256518 miscalculated calloc() during dlclose/tsorting can result in segv
130 4254171 DT_SPARC_REGISTER has invalid value associated with it.
131 -----
132 All the above changes are incorporated in the following patches:
133     Solaris/SunOS 5.7_sparc      patch 106950-07
134     Solaris/SunOS 5.7_x86       patch 106951-07
135     Solaris/SunOS 5.6_sparc     patch 107733-04 (never released)
136     Solaris/SunOS 5.6_x86      patch 107734-04
137 -----
138 4293159 ld needs to combine sections with and without SHF_ORDERED flag(comdat)
139 4292238 linking a library which has a static char ptr invokes mprotect() call
140 -----
141 All the above changes except for:
142 4256518 miscalculated calloc() during dlclose/tsorting can result in segv
143 4254171 DT_SPARC_REGISTER has invalid value associated with it.
144 plus:
145 4238973 fix for 4121152 affects linking of Ada objects
146 4158744 patch 103627-02 causes core when RPATH has blank entry and
147     dlopen/dlclose is used
148 are incorporated in the following patches:
149     Solaris/SunOS 5.5.1_sparc    patch 103627-13
150     Solaris/SunOS 5.5.1_x86     patch 103628-12
151 -----
152 All the above changes are incorporated in the following patches:
153     Solaris/SunOS 5.7_sparc      patch 106950-08
154     Solaris/SunOS 5.7_x86       patch 106951-08
155     Solaris/SunOS 5.6_sparc     patch 107733-05
156     Solaris/SunOS 5.6_x86      patch 107734-05
157 -----
158 4295613 COMMON symbol resolution can be incorrect
159 -----
160 All the above changes plus:
161 4238973 fix for 4121152 affects linking of Ada objects
162 4158744 patch 103627-02 causes core when RPATH has blank entry and
163     dlopen/dlclose is used
164 are incorporated in the following patches:
165     Solaris/SunOS 5.5.1_sparc    patch 103627-14
166     Solaris/SunOS 5.5.1_x86     patch 103628-13
167 -----
168 All the above changes plus:
169 4351197 nfs performance problem by 103627-13
170 are incorporated in the following patches:
171     Solaris/SunOS 5.5.1_sparc    patch 103627-15
172     Solaris/SunOS 5.5.1_x86     patch 103628-14
173 -----
174 All the above changes are incorporated in the following patches:
175     Solaris/SunOS 5.7_sparc      patch 106950-09
176     Solaris/SunOS 5.7_x86       patch 106951-09
177     Solaris/SunOS 5.6_sparc     patch 107733-06
178     Solaris/SunOS 5.6_x86      patch 107734-06
179 -----
180 4158971 increase the default segment alignment for i386 to 64k
181 4064994 Add an $ISALIST token to those understood by the dynamic linker
182 xxxxxxxx ia64 common code putback
183 4239308 LD_DEBUG busted for sparc machines
184 4239008 Support MAP_ANON
185 4238494 link-auditing extensions required
186 4232239 R_SPARC_LOX10 truncates field
187 4231722 R_SPARC_UA* relocations are busted
188 4235514 R_SPARC_OLO10 relocation fails
189 4244025 sgsmg update
190 4239281 need to support SECREL relocations for ia64
191 4253751 ia64 linker must support PT_IA_64_UNWIND tables
192 4259254 dlmopen mistakenly closes fd 0 (stdin) under certain error conditions
193 4260872 libelf hangs when libthread present

```

```

194 4224569 linker core dumping when profiling specified
195 4270937 need mechanism to suppress ld.so.1's use of a default search path.
196 1050476 ld.so to permit configuration of search path
197 4273654 filtee processing using $ISALIST could be optimized
198 4271860 get MERCED cruft out of elf.h
199 4248991 Dynamic loader (via PLT) corrupts register G4
200 4275754 cannot mmap file: Resource temporarily unavailable
201 4277689 The linker can not handle relocation against MOVE tabl
202 4270766 atexit processing required on dlclose().
203 4279229 Add a "release" token to those understood by the dynamic linker
204 4215433 ld can bus error when insufficient disc space exists for output file
205 4285571 Pssst, want some free disk space? ld's miscalculating.
206 4286236 ar gives confusing "bad format" error with a null .stab section
207 4286838 ld.so.1 can't handle a no-bits segment
208 4287364 ld.so.1 runtime configuration cleanup
209 4289573 disable linking of ia64 binaries for Solaris8
210 4293966 crle(1)'s default directories should be supplied
211 -----
213 -----
214 Solaris 8 600 (1st Q-update - s28u1)
215 -----
216 Bugid Risk Synopsis
217 =====
218 4309212 dlsym can't find symbol
219 4311226 rejection of preloading in secure apps is inconsistent
220 4312449 dlclose: invalid deletion of dependency can occur using RTLD_GLOBAL
221 -----
222 All the above changes are incorporated in the following patches:
223     Solaris/SunOS 5.8_sparc      patch 109147-01
224     Solaris/SunOS 5.8_x86       patch 109148-01
225     Solaris/SunOS 5.7_sparc     patch 106950-10
226     Solaris/SunOS 5.7_x86      patch 106951-10
227     Solaris/SunOS 5.6_sparc     patch 107733-07
228     Solaris/SunOS 5.6_x86      patch 107734-07
229 -----
231 -----
232 Solaris 8 900 (2nd Q-update - s28u2)
233 -----
234 Bugid Risk Synopsis
235 =====
236 4324775 non-PIC code & -zcombreloc don't mix very well...
237 4327653 run-time linker should preload tables it will process (madvise)
238 4324324 shared object code can be referenced before .init has fired
239 4321634 .init firing of multiple INITFIRST objects can fail
240 -----
241 All the above changes are incorporated in the following patches:
242     Solaris/SunOS 5.8_sparc      patch 109147-03
243     Solaris/SunOS 5.8_x86       patch 109148-03
244     Solaris/SunOS 5.7_sparc     patch 106950-11
245     Solaris/SunOS 5.7_x86      patch 106951-11
246     Solaris/SunOS 5.6_sparc     patch 107733-08
247     Solaris/SunOS 5.6_x86      patch 107734-08
248 -----
249 4338812 crle(1) omits entries in the directory cache
250 4341496 RFE: provide a static version of /usr/bin/crle
251 4340878 rtdl should treat $ORIGIN like LD_LIBRARY_PATH in security issues
252 -----
253 All the above changes are incorporated in the following patches:
254     Solaris/SunOS 5.8_sparc      patch 109147-04
255     Solaris/SunOS 5.8_x86       patch 109148-04
256     Solaris/SunOS 5.7_sparc     patch 106950-12
257     Solaris/SunOS 5.7_x86      patch 106951-12
258 -----
259 4349563 auxiliary filter error handling regression introduced in 4165487

```

```

260 4355795 ldd -r now gives "displacement relocated" warnings
261 -----
262 All the above changes are incorporated in the following patches:
263   Solaris/SunOS 5.7_sparc      patch 106950-13
264   Solaris/SunOS 5.7_x86       patch 106951-13
265   Solaris/SunOS 5.6_sparc     patch 107733-09
266   Solaris/SunOS 5.6_x86      patch 107734-09
267 -----
268 4210412 versioning a static executable causes ld to core dump
269 4219652 Linker gives misleading error about not finding main (xarch=v9)
270 4103449 ld command needs a command line flag to force 64-bits
271 4187211 problem with RDISP32 linking in copy-relocated objects
272 4287274 dladdr, dlinfo do not provide the full path name of a shared object
273 4297563 dlclose still does not remove all objects.
274 4250694 rtdl_db needs a new auxvec entry
275 4235315 new features for rtdl_db (DT_CHECKSUM, dynamic linked .o files
276 4303609 64bit libelf.so.1 does not properly implement elf_hash()
277 4310901 su.static fails when OSNet build with lazy-loading
278 4310324 elf_errno() causes Bus Error(coredump) in 64-bit multithreaded programs
279 4306415 ld core dump
280 4316531 BCP: possible failure with dlclose/_preexec_exit_handlers
281 4313765 LD_BREADTH should be shot
282 4318162 crle uses automatic strings in putenv.
283 4255943 Description of -t option incomplete.
284 4322528 sgs message test infrastructure needs improvement
285 4239213 Want an API to obtain linker's search path
286 4324134 use of extern mapfile directives can contribute unused symbols
287 4322581 ELF data structures could be layed out more efficiently...
288 4040628 Unnecessary section header symbols should be removed from .dynsym
289 4300018 rtdl: bindlock should be freed before calling call_fini()
290 4336102 dlclose with non-deletable objects can mishandle dependencies
291 4329785 mixing of SHT_SUNW_COMDAT & SHF_ORDERED causes ld to seg fault
292 4334617 COPY relocations should be produces for references to .bss symbols
293 4248250 relocation of local ABS symbols incorrect
294 4335801 For complimentary alignments eliminate ld: warning: symbol 'll'
295         has differing a
296 4336980 ld.so.1 relative path processing revisited
297 4243097 dlderror(3DL) is not affected by setlocale(3C).
298 4344528 dump should remove -D and -l usage message
299 xxxxxxx enable LD_ALTEDEC to access alternate link-editor
300 -----
301 All the above changes are incorporated in the following patches:
302   Solaris/SunOS 5.8_sparc      patch 109147-06
303   Solaris/SunOS 5.8_x86       patch 109148-06
304 -----
306 -----
307 Solaris 8 101 (3rd Q-update - s28u3)
308 -----
309 Bugid    Risk Synopsis
310 =====
311 4346144 link-auditing: plt_tracing fails if LA_SYMB_NOPLTENTER given after
312         being bound
313 4346001 The ld should support mapfile syntax to generate PT_SUNWSTACK segment
314 4349137 rtdl_db: A third fallback method for locating the linkmap
315 4343417 dladdr interface information inadequate
316 4343801 RFE: crle(1): provide option for updating configuration files
317 4346615 ld.so.1 attempting to open a directory gives: No such device
318 4352233 crle should not honor umask
319 4352330 LD_PRELOAD cannot use absolute path for privileged program
320 4357805 RFE: man page for ld(1) does not document all -z or -B options in
321         Solaris 8 9/00
322 4358751 ld.so.1: LD_XXX environ variables and LD_FLAGS should be synchronized.
323 4358862 link editors should reference "64" symlinks instead of sparcv9 (ia64).
324 4356879 PLTs could use faster code sequences in some cases
325 4367118 new fast baplt's fail when traversed twice in threaded application

```

```

326 4366905 Need a way to determine path to a shared library
327 4351197 nfs performance problem by 103627-13
328 4367405 LD_LIBRARY_PATH_64 not being used
329 4354500 SHF_ORDERED ordered sections does not properly sort sections
330 4369068 ld(1)'s weak symbol processing is inefficient (slow and doesn't scale).
331 -----
332 All the above changes are incorporated in the following patches:
333   Solaris/SunOS 5.8_sparc      patch 109147-07
334   Solaris/SunOS 5.8_x86       patch 109148-07
335   Solaris/SunOS 5.7_sparc     patch 106950-14
336   Solaris/SunOS 5.7_x86      patch 106951-14
337 -----
339 -----
340 Solaris 8 701 (5th Q-update - s28u5)
341 -----
342 Bugid    Risk Synopsis
343 =====
344 4368846 ld(1) fails to version some interfaces given in a mapfile
345 4077245 dump core dump on null pointer.
346 4372554 elfdump should demangle symbols (like nm, dump)
347 4371114 dlclose may unmap a promiscuous object while it's still in use.
348 4204447 elfdump should understand SHN_AFTER/SHN_BEGIN macro
349 4377941 initialization of interposers may not occur
350 4381116 ldd/ld.so.1 could aid in detecting unused dependencies
351 4381783 dlopen/dlclose of a libCrun+libthread can dump core
352 4385402 linker & run-time linker must support gABI ELF updates
353 4394698 ld.so.1 does not process DF_SYMBOLIC - not gABI conforming
354 4394212 the link editor quietly ignores missing support libraries
355 4390308 ld.so.1 should provide more flexibility LD_PRELOAD'ing 32-bit/64-bit
356         objects
357 4401232 crle(1) could provide better flexibility for alternatives
358 4401815 fix misc nits in debugging output...
359 4402861 cleanup /usr/demo/link_audit & /usr/tmp/librtdl_db demo source code...
360 4393044 elfdump should allow raw dumping of sections
361 4413168 SHF_ORDERED bit causes linker to generate a separate section
362 -----
363 All the above changes are incorporated in the following patches:
364   Solaris/SunOS 5.8_sparc      patch 109147-08
365   Solaris/SunOS 5.8_x86       patch 109148-08
366 -----
367 4452202 Typos in <sys/link.h>
368 4452220 dump doesn't support RUNPATH
369 -----
370 All the above changes are incorporated in the following patches:
371   Solaris/SunOS 5.8_sparc      patch 109147-09
372   Solaris/SunOS 5.8_x86       patch 109148-09
373 -----
375 -----
376 Solaris 8 1001 (6th Q-update - s28u6)
377 -----
378 Bugid    Risk Synopsis
379 =====
380 4421842 fixups in SHT_GROUP processing required...
381 4450433 problem with liblddbg output on -Dsection,detail when
382         processing SHF_LINK_ORDER
383 -----
384 All the above changes are incorporated in the following patches:
385   Solaris/SunOS 5.8_sparc      patch 109147-10
386   Solaris/SunOS 5.8_x86       patch 109148-10
387   Solaris/SunOS 5.7_sparc     patch 106950-15
388   Solaris/SunOS 5.7_x86      patch 106951-15
389 -----
390 4463473 pldd showing wrong output
391 -----

```

```

392 All the above changes are incorporated in the following patches:
393     Solaris/SunOS 5.8_sparc      patch 109147-11
394     Solaris/SunOS 5.8_x86        patch 109148-11
395 -----
397 -----
398 Solaris 8 202 (7th Q-update - s28u7)
399 -----
400 Bugid    Risk Synopsis
401 =====
402 4488954 ld.so.1 reuses same buffer to send ummapping range to
403     _preexec_exit_handlers()
404 -----
405 All the above changes are incorporated in the following patches:
406     Solaris/SunOS 5.8_sparc      patch 109147-12
407     Solaris/SunOS 5.8_x86        patch 109148-12
408 -----
410 -----
411 Solaris 9
412 -----
413 Bugid    Risk Synopsis
414 =====
415 4505289 incorrect handling of _START_ and _END_
416 4506164 mcs does not recognize #linkbefore or #linkafter qualifiers
417 4447560 strip is creating unexecutable files...
418 4513842 library names not in ld.so string pool cause corefile bugs
419 -----
420 All the above changes are incorporated in the following patches:
421     Solaris/SunOS 5.8_sparc      patch 109147-13
422     Solaris/SunOS 5.8_x86        patch 109148-13
423     Solaris/SunOS 5.7_sparc      patch 106950-16
424     Solaris/SunOS 5.7_x86        patch 106951-16
425 -----
426 4291384 ld -M with a mapfile does not properly align Fortran REAL*8 data
427 4413322 SunOS 5.9 librtld_db doesn't show dlopened ".o" files anymore?
428 4429371 librtld_db busted on ia32 with SC6.x compilers...
429 4418274 elfdump dumps core on invalid input
430 4432224 libelf xlate routines are out of date
431 4433643 Memory leak using dlopen()/dlclose() in Solaris 8
432 4446564 ldd/lddstub - core dump conditions
433 4446115 translating SUNW_move sections is broken
434 4450225 The rdb command can fall into an infinite loop
435 4448531 Linker Causes Segmentation Fault
436 4453241 Regression in 4291384 can result in empty symbol table.
437 4453398 invalid runpath token can cause ld to spin.
438 4460230 ld (for OS 5.8 and 5.9) loses error message
439 4462245 ld.so.1 core dumps when executed directly...
440 4455802 need more flexibility in establishing a support library for ld
441 4467068 dyn_plt_entsize not properly initialized in ld.so.1
442 4468779 elf_plt_trace_write() broken on i386 (link-auditing)
443 4465871 -zld32 and -zld64 does not work the way it should
444 4461890 bad shared object created with -zredlocsym
445 4469400 ld.so.1: is_so_loaded isn't as efficient as we thought...
446 4469566 lazy loading fallback can reference un-relocated objects
447 4470493 libelf incorrectly translates NOTE sections across architectures...
448 4469684 rtdl leaks dl_handles and permits on dlopen/dlclose
449 4475174 ld.so.1 prematurely reports the failure to load a object...
450 4475514 ld.so.1 can core dump in memory allocation fails (no swap)
451 4481851 Setting ld.so.1 environment variables globally would be useful
452 4482035 setting LD_PROFILE & LD_AUDIT causes ping command to issue warnings
453     on 5.8
454 4377735 segment reservations cause sbrk() to fail
455 4491434 ld.so.1 can leak file-descriptors when loading same named objects
456 4289232 some of warning/error/debugging messages from libld.so can be revised
457 4462748 Linker Portion of TLS Support

```

```

458 4496718 run-time linkers mutex_locks not working with ld_libc interface
459 4497270 The -zredlocsym option should not eliminate partially initialized local
460     symbols
461 4496963 dumping an object with crle(1) that uses $ORIGIN can loose its
462     dependencies
463 4499413 Sun linker orders of magnitude slower than gnu linker
464 4461760 lazy loading libXm and libXt can fail.
465 4469031 The partial initialized (local) symbols for intel platform is not
466     working.
467 4492883 Add link-editor option to multi-pass archives to resolve unsatisfied
468     symbols
469 4503731 linker-related commands misspell "argument"
470 4503768 whocalls(1) should output messages to stderr, not stdout
471 4503748 whocalls(1) usage message and manpage could be improved
472 4503625 nm should be taught about TLS symbols - that they aren't allowed that is
473 4300120 segment address validation is too simplistic to handle segment
474     reservations
475 4404547 krtld/reloc.h could have better error message, has typos
476 4270931 R-SPARC_HIX22 relocation is not handled properly
477 4485320 ld needs to support more the 32768 PLTs
478 4516434 sotruss can not watch libc_psr.so.1
479 4213100 sotruss could use more flexible pattern matching
480 4503457 ld seg fault with comdat
481 4510264 sections with SHF_TLS can come in different orders...
482 4518079 link-editor support library unable to modify section header flags
483 4515913 ld.so.1 can incorrectly decrement external reference counts on dlclose()
484 4519569 ld -V does not return a interesting value...
485 4524512 ld.so.1 should allow alternate termination signals
486 4524767 elfdump dies on bogus sh_name fields...
487 4524735 ld getopt processing of '-' changed
488 4521931 subroutine in a shared object as LOCL instead of GLOB
489 -----
490 All the above changes are incorporated in the following patches:
491     Solaris/SunOS 5.8_sparc      patch 109147-14
492     Solaris/SunOS 5.8_x86        patch 109148-14
493     Solaris/SunOS 5.7_sparc      patch 106950-17
494     Solaris/SunOS 5.7_x86        patch 106951-17
495 -----
496 4532729 tentative definition of TLS variable causes linker to dump core
497 4526745 fixup ld error message about duplicate dependencies/needed names
498 4522999 Solaris linker one order of magnitude slower than GNU linker
499 4518966 dldump undoes existing relocations with no thought of alignment or size.
500 4587441 Certain libraries have race conditions when setting error codes
501 4523798 linker option to align bss to large pagesize alignments.
502 4524008 ld can improperly set st_size of symbols named "_init" or "_fini"
503 4619282 ld cannot link a program with the option -sb
504 4620846 Perl Configure probing broken by ld changes
505 4621122 multiple ld '-zinitarray=' on a commandline fails
506 -----
507     Solaris/SunOS 5.8_sparc      patch 109147-15
508     Solaris/SunOS 5.8_x86        patch 109148-15
509     Solaris/SunOS 5.7_sparc      patch 106950-18
510     Solaris/SunOS 5.7_x86        patch 106951-18
511     Solaris/SunOS 5.6_sparc      patch 107733-10
512     Solaris/SunOS 5.6_x86        patch 107734-10
513 -----
514 All the above changes plus:
515 4616944 ar seg faults when order of object file is reversed.
516 are incorporated in the following patches:
517     Solaris/SunOS 5.8_sparc      patch 109147-16
518     Solaris/SunOS 5.8_x86        patch 109148-16
519 -----
520 All the above changes plus:
521 4872634 Large LD_PRELOAD values can cause SEGV of process
522 are incorporated in the following patches:
523     Solaris/SunOS 5.6_sparc      patch T107733-11

```

```

524 Solaris/SunOS 5.6_x86 patch T107734-11
525 -----
527 -----
528 Solaris 9 1202 (2nd Q-update - s9u2)
529 -----
530 Bugid Risk Synopsis
531 =====
532 4546416 add help messages to ld.so mdbmodule
533 4526752 we should build and ship ld.so's mdb module
534 4624658 update 386 TLS relocation values
535 4622472 LA_SYMB_DLSYM not set for la_symbind() invocations
536 4638070 ldd/ld.so.1 could aid in detecting unreferenced dependencies
537 PSARC/2002/096 Detecting unreferenced dependencies with ldd(1)
538 4633860 Optimization for unused static global variables
539 PSARC/2002/113 ld -zignore - section elimination
540 4642829 ld.so.1 mprotect()'s text segment for weak relocations (it shouldn't)
541 4621479 'make' in $SRC/cmd/sgs/tools tries to install things in the proto area
542 4529912 purge ia64 source from sgs
543 4651709 dlopen(RTLD_NOLOAD) can disable lazy loading
544 4655066 crle: -u with nonexistent config file doesn't work
545 4654406 string tables created by the link-editor could be smaller...
546 PSARC/2002/160 ld -znocompstrtab - disable string-table compression
547 4651493 RTLD_NOW can result in binding to an object prior to its init being run.
548 4662575 linker displacement relocation checking introduces significant
549 linker overhead
550 4533195 ld interposes on malloc()/free() preventing support library from freeing
551 memory
552 4630224 crle get's confused about memory layout of objects...
553 4664855 crle on application failed with ld.so.1 encountering mmap() returning
554 ENOMEM err
555 4669582 latest dynamic linker causes libthread_init to get skipped
556 4671493 ld.so.1 inconsistently assigns PATHNAME() on primary objects
557 4668517 compile with map.bssalign doesn't copy _iob to bss
558 -----
559 All the above changes are incorporated in the following patches:
560 Solaris/SunOS 5.9_sparc patch T112963-01
561 Solaris/SunOS 5.8_sparc patch T109147-17
562 Solaris/SunOS 5.8_x86 patch T109148-17
563 -----
564 4701749 On Solaris 8 + 109147-16 ld crashes when building a dynamic library.
565 4707808 The ldd command is broken in the latest 2.8 linker patch.
566 -----
567 All the above changes are incorporated in the following patches:
568 Solaris/SunOS 5.9_sparc patch T112963-02
569 Solaris/SunOS 5.8_sparc patch T109147-18
570 Solaris/SunOS 5.8_x86 patch T109148-18
571 -----
572 4696204 enable extended section indexes in relocatable objects
573 PSARC/2001/332 ELF gABI updates - round II
574 PSARC/2002/369 libelf interfaces to support ELF Extended Sections
575 4706503 linkers need to cope with EF_SPARCV9_PSO/EF_SPARCV9_RMO
576 4716929 updating of local register symbols in dynamic sytab busted...
577 4710814 add "official" support for the "symbolic" keyword in linker map-file
578 PSARC/2002/439 linker mapfile visibility declarations
579 -----
580 All the above changes are incorporated in the following patches:
581 Solaris/SunOS 5.9_sparc patch T112963-03
582 Solaris/SunOS 5.8_sparc patch T109147-19
583 Solaris/SunOS 5.8_x86 patch T109148-19
584 Solaris/SunOS 5.7_sparc patch T106950-19
585 Solaris/SunOS 5.7_x86 patch T106951-19
586 -----
588 -----
589 Solaris 9 403 (3rd Q-update - s9u3)

```

```

590 -----
591 Bugid Risk Synopsis
592 =====
593 4731174 strip(1) does not fixup SHT_GROUP data
594 4733697 -zignore with gcc may exclude C++ exception sections
595 4733317 R_SPARC*_HIX22 calculations are wrong with 32bit LD building
596 ELF64 binaries
597 4735165 fatal linker error when compiling C++ programs with -xlinkopt
598 4736951 The mcs broken when the target file is an archive file
599 -----
600 All the above changes are incorporated in the following patches:
601 Solaris/SunOS 5.8_sparc patch T109147-20
602 Solaris/SunOS 5.8_x86 patch T109148-20
603 Solaris/SunOS 5.7_sparc patch T106950-20
604 Solaris/SunOS 5.7_x86 patch T106951-20
605 -----
606 4739660 Threads deadlock in schedlock and dynamic linker lock.
607 4653148 ld.so.1/libc should unregister its dlclose() exit handler via a fini.
608 4743413 ld.so.1 doesn't terminate argv with NULL pointer when invoked directly
609 4746231 linker core-dumps when SECTION relocations are made against discarded
610 sections
611 4730433 ld.so.1 wastes time repeatedly opening dependencies
612 4744337 missing RD_CONSISTENT event with dlopen(LD_ID_NEWLM, ...)
613 4670835 rd_load_objiter can ignore callback's return value
614 4745932 strip utility doesn't strip out Dwarf2 debug section
615 4754751 "strip" command doesn't remove comdat stab sections.
616 4755674 Patch 109147-18 results in coredump.
617 -----
618 All the above changes are incorporated in the following patches:
619 Solaris/SunOS 5.9_sparc patch T112963-04
620 Solaris/SunOS 5.7_sparc patch T106950-21
621 Solaris/SunOS 5.7_x86 patch T106951-21
622 -----
623 4772927 strip core dumps on an archive library
624 4774727 direct-bindings can fail against copy-reloc symbols
625 -----
626 All the above changes are incorporated in the following patches:
627 Solaris/SunOS 5.9_sparc patch T112963-05
628 Solaris/SunOS 5.9_x86 patch T113986-01
629 Solaris/SunOS 5.8_sparc patch T109147-21
630 Solaris/SunOS 5.8_x86 patch T109148-21
631 Solaris/SunOS 5.7_sparc patch T106950-22
632 Solaris/SunOS 5.7_x86 patch T106951-22
633 -----
635 -----
636 Solaris 9 803 (4th Q-update - s9u4)
637 -----
638 Bugid Risk Synopsis
639 =====
640 4730110 ld.so.1 list implementation could scale better
641 4728822 restrict the objects dlsym() searches.
642 PSARC/2002/478 New dlopen(3dl) flag - RTLD_FIRST
643 4714146 crle: 64-bit secure pathname is incorrect.
644 4504895 dlclose() does not remove all objects
645 4698800 Wrong comments in /usr/lib/ld/sparcv9/map.*
646 4745129 dldump is inconsistent with .dynamic processing errors.
647 4753066 LD_SIGNAL isn't very useful in a threaded environment
648 PSARC/2002/569 New dldinfo(3dl) flag - RTLD_DI_SIGNAL
649 4765536 crle: symbolic links can confuse alternative object configuration info
650 4766815 ld -r of object the TLS data fails
651 4770484 elfdump can not handle stripped archive file
652 4770494 The ld command gives improper error message handling broken archive
653 4775738 overwriting output relocation table when 'ld -zignore' is used
654 4778247 elfdump -e of core files fails
655 4779976 elfdump dies on bad relocation entries

```

```

656 4787579 invalid SHT_GROUP entries can cause linker to seg fault
657 4783869 dlclose: filter closure exhibits hang/failure - introduced with 4504895
658 4778418 ld.so.1: there be nits out there
659 4792461 Thread-Local Storage - x86 instruction sequence updates
660 PSARC/2002/746 Thread-Local Storage - x86 instruction sequence updates
661 4461340 sgs: ugly build output while suppressing ia64 (64-bit) build on Intel
662 4790194 dlopen(..., RTLD_GROUP) has an odd interaction with interposition
663 4804328 auditing of threaded applications results in deadlock
664 4806476 building relocatable objects with SHF_EXCLUDE loses relocation
665 information
666 -----
667 All the above changes are incorporated in the following patches:
668 Solaris/SunOS 5.9_sparc patch T112963-06
669 Solaris/SunOS 5.9_x86 patch T113986-02
670 Solaris/SunOS 5.8_sparc patch T109147-22
671 Solaris/SunOS 5.8_x86 patch T109148-22
672 -----
673 4731183 compiler creates .tlsbss section instead of .tbss as documented
674 4816378 TLS: a tls test case dumps core with C and C++ compilers
675 4817314 TLS_GD relocations against local symbols do not reference symbol...
676 4811951 non-default symbol visibility overridden by definition in shared object
677 4802194 relocation error of mozilla built by K2 compiler
678 4715815 ld should allow linking with no output file (or /dev/null)
679 4793721 Need a way to null all code in ISV objects enabling ld performance
680 tuning
681 -----
682 All the above changes plus:
683 4796237 RFE: link-editor became extremely slow with patch 109147-20 and
684 static libraries
685 are incorporated in the following patches:
686 Solaris/SunOS 5.9_sparc patch T112963-07
687 Solaris/SunOS 5.9_x86 patch T113986-03
688 Solaris/SunOS 5.8_sparc patch T109147-23
689 Solaris/SunOS 5.8_x86 patch T109148-23
690 -----
691 -----
692 -----
693 Solaris 9 1203 (5th Q-update - s9u5)
694 -----
695 Bugid Risk Synopsis
696 =====
697 4830584 mmap for the padding region doesn't get freed after dlclose
698 4831650 ld.so.1 can walk off the end of it's call_init() array...
699 4831544 ldd using .so modules compiled with FD7 compiler caused a core dump
700 4834784 Accessing members in a TLS structure causes a core dump in Oracle
701 4824026 segv when -z combrelloc is used with -xlkopt
702 4825296 typo in elfdump
703 -----
704 All the above changes are incorporated in the following patches:
705 Solaris/SunOS 5.9_sparc patch T112963-08
706 Solaris/SunOS 5.9_x86 patch T113986-04
707 Solaris/SunOS 5.8_sparc patch T109147-24
708 Solaris/SunOS 5.8_x86 patch T109148-24
709 -----
710 4470917 Solaris Process Model Unification (link-editor components only)
711 PSARC/2002/117 Solaris Process Model Unification
712 4744411 Bloomberg wants a faster linker.
713 4811969 64-bit links can be much slower than 32-bit.
714 4825065 ld(1) should ignore consecutive empty sections.
715 4838226 unrellocated shared objects may be erroneously collected for init firing
716 4830889 TLS: testcase coredumps with -xarch=v9 and -g
717 4845764 filter removal can leave dangling filtee pointer
718 4811093 appttrace -F libc date core dumps
719 4826315 Link editors need to be pre- and post- Unified Process Model aware
720 4868300 interposing on direct bindings can fail
721 4872634 Large LD_PRELOAD values can cause SEGV of process

```

```

722 -----
723 All the above changes are incorporated in the following patches:
724 Solaris/SunOS 5.9_sparc patch T112963-09
725 Solaris/SunOS 5.9_x86 patch T113986-05
726 Solaris/SunOS 5.8_sparc patch T109147-25
727 Solaris/SunOS 5.8_x86 patch T109148-25
728 -----
729 -----
730 -----
731 Solaris 9 404 (6th Q-update - s9u6)
732 -----
733 Bugid Risk Synopsis
734 =====
735 4870260 The elfdump command should produce more warning message on invalid move
736 entries.
737 4865418 empty PT_TLS program headers cause problems in TLS enabled applications
738 4825151 compiler core dumped with a -mt -xF=%all test
739 4845829 The runtime linker fails to dlopen() long path name.
740 4900684 shared libraries with more than 32768 plt's fail for sparc ELF64
741 4906062 Makefiles under usr/src/cmd/sgs needs to be updated
742 -----
743 All the above changes are incorporated in the following patches:
744 Solaris/SunOS 5.9_sparc patch T112963-10
745 Solaris/SunOS 5.9_x86 patch T113986-06
746 Solaris/SunOS 5.8_sparc patch T109147-26
747 Solaris/SunOS 5.8_x86 patch T109148-26
748 Solaris/SunOS 5.7_sparc patch T106950-24
749 Solaris/SunOS 5.7_x86 patch T106951-24
750 -----
751 4900320 rtdl library mapping could be faster
752 4911775 implement GOTDATA proposal in ld
753 PSARC/2003/477 SPARC GOTDATA instruction sequences
754 4904565 Functionality to ignore relocations against external symbols
755 4764817 add section types SHT_DEBUG and SHT_DEBUGSTR
756 PSARC/2003/510 New ELF DEBUG and ANNOTATE sections
757 4850703 enable per-symbol direct bindings
758 4716275 Help required in the link analysis of runtime interfaces
759 PSARC/2003/519 Link-editors: Direct Binding Updates
760 4904573 elfdump may hang when processing archive files
761 4918310 direct binding from an executable can't be interposed on
762 4918938 ld.so.1 has become SPARC32PLUS - breaks 4.x binary compatibility
763 4911796 S1S8 C++: ld dump core when compiled and linked with xlkopt=1.
764 4889914 ld crashes with SEGV using -M mapfile under certain conditions
765 4911936 exception are not catch from shared library with -zignore
766 -----
767 All the above changes are incorporated in the following patches:
768 Solaris/SunOS 5.9_sparc patch T112963-11
769 Solaris/SunOS 5.9_x86 patch T113986-07
770 Solaris/SunOS 5.8_sparc patch T109147-27
771 Solaris/SunOS 5.8_x86 patch T109148-27
772 Solaris/SunOS 5.7_sparc patch T106950-25
773 Solaris/SunOS 5.7_x86 patch T106951-25
774 -----
775 4946992 ld crashes due to huge number of sections (>65,000)
776 4951840 mcs -c goes into a loop on executable program
777 4939869 Need additional relocation types for abs34 code model
778 PSARC/2003/684 abs34 ELF relocations
779 -----
780 All the above changes are incorporated in the following patches:
781 Solaris/SunOS 5.9_sparc patch T112963-12
782 Solaris/SunOS 5.9_x86 patch T113986-08
783 Solaris/SunOS 5.8_sparc patch T109147-28
784 Solaris/SunOS 5.8_x86 patch T109148-28
785 -----
786 -----
787 -----

```

```

788 Solaris 9 904 (7th Q-update - s9u7)
789 -----
790 Bugid Risk Synopsis
791 =====
792 4912214 Having multiple of libc.so.1 in a link map causes malloc() to fail
793 4526878 ld.so.1 should pass MAP_ALIGN flag to give kernel more flexibility
794 4930997 sgs_bld_vernote.ksh script needs to be hardend...
795 4796286 ld.so.1: scenario for trouble?
796 4930985 clean up cruft under usr/src/cmd/sgs/tools
797 4933300 remove references to Ultra-1 in librtld_db demo
798 4936305 string table compression is much too slow...
799 4939626 SUNWonld internal package must be updated...
800 4939565 per-symbol filtering required
801 4948119 ld(1) -z loadfltr fails with per-symbol filtering
802 4948427 ld.so.1 gives fatal error when multiple RTLDINFO objects are loaded
803 4940894 ld core dumps using "-xldscope=symbolic
804 4955373 per-symbol filtering refinements
805 4878827 crle(1M) - display post-UPM search paths, and compensate for pre-UPM.
806 4955802 /usr/ccs/bin/ld dumps core in process_reld()
807 4964415 elfdump issues wrong relocation error message
808 4966465 LD_NOAUXFLTR fails when object is both a standard and auxiliary filter
809 4973865 the link-editor does not scale properly when linking objects with
810 lots of syms
811 4975598 SHT_SUNW_ANNOTATE section relocation not resolved
812 4974828 nss_files nss_compat r_mt tests randomly segfaulting
813 -----
814 All the above changes are incorporated in the following patches:
815 Solaris/SunOS 5.9_sparc patch T112963-13
816 Solaris/SunOS 5.9_x86 patch T113986-09
817 -----
818 4860508 link-editors should create/promote/verify hardware capabilities
819 5002160 crle: reservation for dumped objects gets confused by mmaped object
820 4967869 linking stripped library causes segv in linker
821 5006657 link-editor doesn't always handle nodirect binding syminfo information
822 4915901 no way to see ELF information
823 5021773 ld.so.1 has trouble with objects having more than 2 segments.
824 -----
825 All the above changes are incorporated in the following patches:
826 Solaris/SunOS 5.9_sparc patch T112963-14
827 Solaris/SunOS 5.9_x86 patch T113986-10
828 Solaris/SunOS 5.8_sparc patch T109147-29
829 Solaris/SunOS 5.8_x86 patch T109148-29
830 -----
831 All the above changes plus:
832 6850124 dlopen reports "No such file or directory" in spite of ENOMEM
833 when mmap fails in anon_map()
834 are incorporated in the following patches:
835 Solaris/SunOS 5.9_sparc patch TXXXXXX-XX
836 Solaris/SunOS 5.9_x86 patch TXXXXXX-XX
837 -----
839 -----
840 Solaris 10
841 -----
842 Bugid Risk Synopsis
843 =====
844 5044797 ld.so.1: secure directory testing is being skipped during filtee
845 processing
846 4963676 Remove remaining static libraries
847 5021541 unnecessary PT_SUNWBSS segment may be created
848 5031495 elfdump complains about bad symbol entries in core files
849 5012172 Need error when creating shared object with .o compiled
850 -xarch=v9 -xcode=abs44
851 4994738 rd_plt_resolution() resolves ebx-relative PLT entries incorrectly
852 5023493 ld -m output with patch 109147-25 missing .o information
853 -----

```

```

854 All the above changes are incorporated in the following patches:
855 Solaris/SunOS 5.9_sparc patch T112963-15
856 Solaris/SunOS 5.9_x86 patch T113986-11
857 Solaris/SunOS 5.8_sparc patch T109147-30
858 Solaris/SunOS 5.8_x86 patch T109148-30
859 -----
860 5071614 109147-29 & -30 break the build of on28-patch on Solaris 8 2/04
861 5029830 crle: provide for optional alternative dependencies.
862 5034652 ld.so.1 should save, and print, more error messages
863 5036561 ld.so.1 outputs non-fatal fatal message about auxiliary filter libraries
864 5042713 4866170 broke ld.so's ::setenv
865 5047082 ld can core dump on bad gcc objects
866 5047612 ld.so.1: secure pathname verification is flawed with filter use
867 5047235 elfdump can core dump printing PT_INTERP section
868 4798376 nits in demo code
869 5041446 gelf_update.*( ) functions inconsistently return NULL or 0
870 5032364 M_ID_TLSBSS and M_ID_UNKNOWN have the same value
871 4707030 Empty LD_PRELOAD_64 doesn't override LD_PRELOAD
872 4968618 symbolic linkage causes core dump
873 5062313 dladdr() can cause deadlock in MT apps.
874 5056867 $SALIST/$HWCAP expansion should be more flexible.
875 4918303 000.so.1 should not use compiler-supplied crt*.o files
876 5058415 whocalls cannot take more than 10 arguments
877 5067518 The fix for 4918303 breaks the build if a new work space is used.
878 -----
879 All the above changes are incorporated in the following patches:
880 Solaris/SunOS 5.9_sparc patch T112963-16
881 Solaris/SunOS 5.9_x86 patch T113986-12
882 Solaris/SunOS 5.8_sparc patch T109147-31
883 Solaris/SunOS 5.8_x86 patch T109148-31
884 -----
885 5013759 *file* should report hardware/software capabilities (link-editor
886 components only)
887 5063580 libldstab: file /tmp/posto... .stab[.index|.sbfocus] found with no
888 matching stri
889 5076838 elfdump(1) is built with a CTF section (the wrong one)
890 5080344 Hardware capabilities are not enforced for a.out
891 5079061 RTLD_DEFAULT can be expensive
892 PSARC/2004/747 New dlSYM(3C) Handle - RTLD_PROBE
893 5064973 allow normal relocations against TLS symbols for some sections
894 5085792 LD_XXXX_64 should override LD_XXXX
895 5096272 every executable or library has a .SUNW_dof section
896 5094135 Bloomberg wants a faster ldd.
897 5086352 libld.so.3 should be built with a .SUNW_ctf ELF section, ready for CR
898 5098205 elfdump gives wrong section name for the global offset table
899 5092414 Linker patch 109147-29 makes Broadvision One-To-One server v4.1
900 installation fail
901 5080256 dump(1) doesn't list ELF hardware capabilities
902 5097347 recursive read lock in gelf_getsym()
903 -----
904 All the above changes are incorporated in the following patches:
905 Solaris/SunOS 5.9_sparc patch T112963-17
906 Solaris/SunOS 5.9_x86 patch T113986-13
907 Solaris/SunOS 5.8_sparc patch T109147-32
908 Solaris/SunOS 5.8_x86 patch T109148-32
909 -----
910 5106206 ld.so.1 fail to run a Solaris9 program that has libc linked with
911 -z lazyload
912 5102601 ON should deliver a 64-bit operating system for Opteron systems
913 (link-editor components only)
914 6173852 enable link_auditing technology for amd64
915 6174599 linker does not create .eh_frame_hdr sections for eh_frame sections
916 with SHF_LINK_ORDER
917 6175609 amd64 run-time linker has a corrupted note section
918 6175843 amd64 rdb_demo files not installed
919 6182293 ld.so.1 can repeatedly relocate object .plats (RTLD_NOW).

```

```

920 6183645 ld core dumps when automounter fails
921 6178667 ldd list unexpected (file not found) in x86 environment.
922 6181928 Need new reloc types R_AMD64_GOTOFF64 and R_AMD64_GOTPC32
923 6182884 AMD64: ld core dumps when building a shared library
924 6173559 The ld may set incorrect value for sh_addralign under some conditions.
925 5105601 ld.so.1 gets a little too enthusiastic with interposition
926 6189384 ld.so.1 should accommodate a files dev/inode change (libc loopback mnt)
927 6177838 AMD64: linker cannot resolve PLT for 32-bit a.out(s) on amd64-S2 kernel
928 6190863 sparc disassembly code should be removed from rdb_demo
929 6191488 unwind eh_frame_hdr needs corrected encoding value
930 6192490 moe(1) returns /lib/libc.so.1 for optimal expansion of libc HWCAP
931 libraries
932 6192164 AMD64: introduce dlamd64getunwind interface
933 PSARC/2004/747 libc::dlamd64getunwind()
934 6195030 libldl has bad version name
935 6195521 64-bit moe(1) missed the train
936 6198358 AMD64: bad eh_frame_hdr data when C and C++ mixed in a.out
937 6204123 ld.so.1: symbol lookup fails even after lazy loading fallback
938 6207495 UNIX98/UNIX03 vsx namespace violation DYNL.hdr/misc/dlfcn/T.dlfcn
939 14 Failed
940 6217285 ctfmerge crashed during full onnv build
941 -----

943 -----
944 Solaris 10 106 (1st Q-update - s10u1)
945 -----
946 Bugid Risk Synopsis
947 =====
948 6209350 Do not include signature section from dynamic dependency library into
949 relocatable object
950 6212797 The binary compiled on SunOS4.x doesn't run on Solaris8 with Patch
951 109147-31
952 -----
953 All the above changes are incorporated in the following patches:
954 Solaris/SunOS 5.9_sparc patch T112963-18
955 Solaris/SunOS 5.9_x86 patch T113986-14
956 Solaris/SunOS 5.8_sparc patch T109147-33
957 Solaris/SunOS 5.8_x86 patch T109148-33
958 -----
959 6219538 112963-17: linker patch causes binary to dump core
960 -----
961 All the above changes are incorporated in the following patches:
962 Solaris/SunOS 5.10_sparc patch T117461-01
963 Solaris/SunOS 5.10_x86 patch T118345-01
964 Solaris/SunOS 5.9_sparc patch T112963-19
965 Solaris/SunOS 5.9_x86 patch T113986-15
966 Solaris/SunOS 5.8_sparc patch T109147-34
967 Solaris/SunOS 5.8_x86 patch T109148-34
968 -----
969 6257177 incremental builds of usr/src/cmd/sgs can fail...
970 6219651 AMD64: Linker does not issue error for out of range R_AMD64_PC32
971 -----
972 All the above changes are incorporated in the following patches:
973 Solaris/SunOS 5.10_sparc patch T117461-02
974 Solaris/SunOS 5.10_x86 patch T118345-02
975 Solaris/SunOS 5.9_sparc patch T112963-20
976 Solaris/SunOS 5.9_x86 patch T113986-16
977 Solaris/SunOS 5.8_sparc patch T109147-35
978 Solaris/SunOS 5.8_x86 patch T109148-35
979 NOTE: The fix for 6219651 is only applicable for 5.10_x86 platform.
980 -----
981 5080443 lazy loading failure doesn't clean up after itself (D)
982 6226206 ld.so.1 failure when processing single segment hwcapi filter
983 6228472 ld.so.1: link-map control list stacking can loose objects
984 6235000 random packages not getting installed in snv_09 and snv_10 -
985 rld/common/malloc.c Assertion

```

```

986 6219317 Large page support is needed for mapping executables, libraries and
987 files (link-editor components only)
988 6244897 ld.so.1 can't run apps from commandline
989 6251798 moe(1) returns an internal assertion failure message in some
990 circumstances
991 6251722 ld fails silently with exit 1 status when -z ignore passed
992 6254364 ld won't build libgenunix.so with absolute relocations
993 6215444 ld.so.1 caches "not there" lazy libraries, foils svc.startd(1M)'s logic
994 6222525 dlsym(3C) trusts caller(), which may return wrong results with tail call
995 optimization
996 6241995 warnings in sgs should be fixed (link-editor components only)
997 6258834 direct binding availability should be verified at runtime
998 6260361 lari shouldn't count a.out non-zero undefined entries as interesting
999 6260780 ldd doesn't recognize LD_NOAUXFLTR
1000 6266261 Add ld(1) -Bnoirect support (D)
1001 6261990 invalid e_flags error could be a little more friendly
1002 6261803 lari(1) should find more events uninteresting (D)
1003 6267352 libld_malloc provides inadequate alignment
1004 6268693 SHN_SUNW_IGNORE symbols should be allowed to be multiply defined
1005 6262789 Infosys wants a faster linker
1006 -----
1007 All the above changes are incorporated in the following patches:
1008 Solaris/SunOS 5.10_sparc patch T117461-03
1009 Solaris/SunOS 5.10_x86 patch T118345-03
1010 Solaris/SunOS 5.9_sparc patch T112963-21
1011 Solaris/SunOS 5.9_x86 patch T113986-17
1012 Solaris/SunOS 5.8_sparc patch T109147-36
1013 Solaris/SunOS 5.8_x86 patch T109148-36
1014 -----
1015 6283601 The usr/src/cmd/sgs/packages/common/copyright contains old information
1016 legally problematic
1017 6276905 dlinfo gives inconsistent results (relative vs absolute linkname) (D)
1018 PSARC/2005/357 dlinfo(3c) RTLD_DI_ARGINFO
1019 6284941 excessive link times with many groups/sections
1020 6280467 dlclose() unmaps shared library before library's _fini() has finished
1021 6291547 ld.so mishandles LD_AUDIT causing security problems.
1022 -----
1023 All the above changes are incorporated in the following patches:
1024 Solaris/SunOS 5.10_sparc patch T117461-04
1025 Solaris/SunOS 5.10_x86 patch T118345-04
1026 Solaris/SunOS 5.9_sparc patch T112963-22
1027 Solaris/SunOS 5.9_x86 patch T113986-18
1028 Solaris/SunOS 5.8_sparc patch T109147-37
1029 Solaris/SunOS 5.8_x86 patch T109148-37
1030 -----
1031 6295971 UNIX98/UNIX03 *vsx* DYNL.hdr/misc/dlfcn/T.dlfcn 14 fails, auxv.h syntax
1032 error
1033 6299525 .init order failure when processing cycles
1034 6273855 gcc and sgs/crle don't get along
1035 6273864 gcc and sgs/libld don't get along
1036 6273875 gcc and sgs/rtld don't get along
1037 6272563 gcc and amd64/krtld/doreloc.c don't get along
1038 6290157 gcc and sgs/librtld_db/rdb_demo don't get along
1039 6301218 Matlab dumps core on startup when running on 112963-22 (D)
1040 -----
1041 All the above changes are incorporated in the following patches:
1042 Solaris/SunOS 5.10_sparc patch T117461-06
1043 Solaris/SunOS 5.10_x86 patch T118345-08
1044 Solaris/SunOS 5.9_sparc patch T112963-23
1045 Solaris/SunOS 5.9_x86 patch T113986-19
1046 Solaris/SunOS 5.8_sparc patch T109147-38
1047 Solaris/SunOS 5.8_x86 patch T109148-38
1048 -----
1049 6314115 Checkpoint refuses to start, crashes on start, after application of
1050 linker patch 112963-22
1051 -----

```

```

1052 All the above changes are incorporated in the following patches:
1053 Solaris/SunOS 5.9_sparc patch T112963-24
1054 Solaris/SunOS 5.9_x86 patch T113986-20
1055 Solaris/SunOS 5.8_sparc patch T109147-39
1056 Solaris/SunOS 5.8_x86 patch T109148-39
1057 -----
1058 6318306 a dlsym() from a filter should be redirected to an associated filtee
1059 6318401 mis-aligned TLS variable
1060 6324019 ld.so.1: malloc alignment is insufficient for new compilers
1061 6324589 psh coredumps on x86 machines on snv_23
1062 6236594 AMD64: Linker needs to handle the new .lbss section (D)
1063 PSARC 2005/514 AMD64 - large section support
1064 6314743 Linker: incorrect resolution for R_AMD64_GOTPC32
1065 6311865 Linker: x86 medium model; invalid ELF program header
1066 -----
1067 All the above changes are incorporated in the following patches:
1068 Solaris/SunOS 5.10_sparc patch T117461-07
1069 Solaris/SunOS 5.10_x86 patch T118345-12
1070 -----
1071 6309061 link_audit should use __asm__ with gcc
1072 6310736 gcc and sgs/libld don't get along on SPARC
1073 6329796 Memory leak with iconv_open/iconv_close with patch 109147-33
1074 6332983 s9 linker patches 112963-24/113986-20 causing cluster machines not
1075 to boot
1076 -----
1077 All the above changes are incorporated in the following patches:
1078 Solaris/SunOS 5.10_sparc patch T117461-08
1079 Solaris/SunOS 5.10_x86 patch T121208-02
1080 Solaris/SunOS 5.9_sparc patch T112963-25
1081 Solaris/SunOS 5.9_x86 patch T113986-21
1082 Solaris/SunOS 5.8_sparc patch T109147-40
1083 Solaris/SunOS 5.8_x86 patch T109148-40
1084 -----
1085 6445311 The sparc S8/S9/S10 linker patches which include the fix for the
1086 CR6222525 are hit by the CR6439613.
1087 -----
1088 All the above changes are incorporated in the following patches:
1089 Solaris/SunOS 5.9_sparc patch T112963-26
1090 Solaris/SunOS 5.8_sparc patch T109147-41
1091 -----
1093 -----
1094 Solaris 10 807 (4th Q-update - s10u4)
1095 -----
1096 Bugid Risk Synopsis
1097 =====
1098 6487273 ld.so.1 may open arbitrary locale files when relative path is built
1099 from locale environment vars
1100 6487284 ld.so.1: buffer overflow in doprf() function
1101 -----
1102 All the above changes are incorporated in the following patches:
1103 Solaris/SunOS 5.10_sparc patch T124922-01
1104 Solaris/SunOS 5.10_x86 patch T124923-01
1105 Solaris/SunOS 5.9_sparc patch T112963-27
1106 Solaris/SunOS 5.9_x86 patch T113986-22
1107 Solaris/SunOS 5.8_sparc patch T109147-42
1108 Solaris/SunOS 5.8_x86 patch T109148-41
1109 -----
1110 6477132 ld.so.1: memory leak when running set*id application
1111 -----
1112 All the above changes are incorporated in the following patches:
1113 Solaris/SunOS 5.10_sparc patch T124922-02
1114 Solaris/SunOS 5.10_x86 patch T124923-02
1115 Solaris/SunOS 5.9_sparc patch T112963-30
1116 Solaris/SunOS 5.9_x86 patch T113986-24
1117 -----

```

```

1118 6340814 ld.so.1 core dump with HWCAP relocatable object + updated statistics
1119 6307274 crle bug with LD_LIBRARY_PATH
1120 6317969 elfheader limited to 65535 segments (link-editor components only)
1121 6350027 ld.so.1 aborts with assertion failed on amd64
1122 6362044 ld(1) inconsistencies with LD_DEBUG-Dunused and -zignore
1123 6362047 ld.so.1 dumps core when combining HWCAP and LD_PROFILE
1124 6304206 runtime linker may respect LANG and LC_MESSAGE more than LC_ALL
1125 6363495 Catchup required with Intel relocations
1126 6326497 ld.so not properly processing LD_LIBRARY_PATH ending in :
1127 6307146 mcs dumps core when appending null string to comment section
1128 6371877 LD_PROFILE_64 with gprof does not produce correct results on amd64
1129 6372082 ld -r erroneously creates .got section on i386
1130 6201866 amd64: linker symbol elimination is broken
1131 6372620 printstack() segfaults when called from static function (D)
1132 6380470 32-bit ld(1) incorrectly builds 64-bit relocatable objects
1133 6391407 Insufficient alignment of 32-bit object in archive makes ld segfault
1134 (libelf component only) (D)
1135 6316708 LD_DEBUG should provide a means of identifying/isolating individual
1136 link-map lists (P)
1137 6280209 elfdump cores on memory model 0x3
1138 6197234 elfdump and dump don't handle 64-bit symbols correctly
1139 6398893 Extended section processing needs some work
1140 6397256 ldd dumps core in elf_fix_name
1141 6327926 ld does not set etext symbol correctly for AMD64 medium model (D)
1142 6390410 64-bit LD_PROFILE can fail: relocation error when binding profile plt
1143 6382945 AMD64-GCC: dbx: internal error: dwarf reference attribute out of bounds
1144 6262333 init section of .so dlopened from audit interface not being called
1145 6409613 elf_outsync() should fsync()
1146 6426048 C++ exceptions broken in Nevada for amd64
1147 6429418 ld.so.1: need work-around for Nvidia drivers use of static TLS
1148 6429504 crle(1) shows wrong defaults for non-existent 64-bit config file
1149 6431835 data corruption on x64 in 64-bit mode while LD_PROFILE is in effect
1150 6423051 static TLS support within the link-editors needs a major face lift (D)
1151 6388946 attempting to dlopen a .o file mislabeled as .so fails
1152 6446740 allow mapfile symbol definitions to create backing storage (D)
1153 4986360 linker crash on exec of .so (as opposed to a.out) -- error preferred
1154 instead
1155 6229145 ld: initarray/finiarray processing occurs after got size is determined
1156 6324924 the linker should warn if there's a .init section but not _init
1157 6424132 elfdump inserts extra whitespace in bitmap value display
1158 6449485 ld(1) creates misaligned TLS in binary compiled with -xpg
1159 6424550 Write to unallocated (wua) errors when libraries are built with
1160 -z lazyload
1161 6464235 executing the 64-bit ld(1) should be easy (D)
1162 6465623 need a way of building unix without an interpreter
1163 6467925 ld: section deletion (-z ignore) requires improvement
1164 6357230 specfiles should be nuked (link-editor components only)
1165 -----
1166 All the above changes are incorporated in the following patches:
1167 Solaris/SunOS 5.10_sparc patch T124922-03
1168 Solaris/SunOS 5.10_x86 patch T124923-03
1169 -----
1170 These patches also include the framework changes for the following bug fixes.
1171 However, the associated feature has not been enabled in Solaris 10 or earlier
1172 releases:
1173 -----
1174 6174390 crle configuration files are inconsistent across platforms (D, P)
1175 6432984 ld(1) output file removal - change default behavior (D)
1176 PSARC/2006/353 ld(1) output file removal - change default behavior
1177 -----
1179 -----
1180 Solaris 10 508 (5th Q-update - s10u5)
1181 -----
1182 Bugid Risk Synopsis
1183 =====

```

```

1184 6561987 data vac_conflict faults on liphthead libthead libs in s10.
1185 -----
1186 All the above changes are incorporated in the following patches:
1187 Solaris/SunOS 5.10_sparc patch T127111-01
1188 Solaris/SunOS 5.10_x86 patch T127112-01
1189 -----
1190 6501793 GOTOP relocation transition (optimization) fails with offsets > 2^32
1191 6532924 AMD64: Solaris 5.11 55b: SEGV after whocatches
1192 6551627 OGL: SIGSEGV when trying to use OpenGL pipeline with splash screen,
1193 Solaris/Nvidia only
1194 -----
1195 All the above changes are incorporated in the following patches:
1196 Solaris/SunOS 5.10_sparc patch T127111-04
1197 Solaris/SunOS 5.10_x86 patch T127112-04
1198 -----
1199 6479848 Enhancements to the linker support interface needed. (D)
1200 PSARC/2006/595 link-editor support library interface - ld_open()
1201 6521608 assertion failure in runtime linker related to auditing
1202 6494228 pclose() error when an audit library calls popen() and the main target
1203 is being run under ldd (D)
1204 6568745 segfault when using LD_DEBUG with bit_audit library when instrumenting
1205 mozilla (D)
1206 PSARC/2007/413 Add -zglobalaudit option to ld
1207 6602294 ps_pbrandname breaks apps linked directly against librtld_db
1208 -----
1209 All the above changes are incorporated in the following patches:
1210 Solaris/SunOS 5.10_sparc patch T127111-07
1211 Solaris/SunOS 5.10_x86 patch T127112-07
1212 -----
1213 -----
1214 -----
1215 Solaris 10 908 (6th Q-update - s10u6)
1216 -----
1217 Bugid Risk Synopsis
1218 =====
1219 6672544 elf_rtbndr must support non-ABI aligned stacks on amd64
1220 6668050 First trip through PLT does not preserve args in xmm registers
1221 -----
1222 All the above changes are incorporated in the following patch:
1223 Solaris/SunOS 5.10_x86 patch T137138-01
1224 -----
1225 -----
1226 -----
1227 Solaris 10 409 (7th Q-update - s10u7)
1228 -----
1229 Bugid Risk Synopsis
1230 =====
1231 6629404 ld with -z ignore doesn't scale
1232 6606203 link editor ought to allow creation of >2gb sized objects (P)
1233 -----
1234 All the above changes are incorporated in the following patches:
1235 Solaris/SunOS 5.10_sparc patch T139574-01
1236 Solaris/SunOS 5.10_x86 patch T139575-01
1237 -----
1238 6746674 setuid applications do not find libraries any more because trusted
1239 directories behavior changed (D)
1240 -----
1241 All the above changes are incorporated in the following patches:
1242 Solaris/SunOS 5.10_sparc patch T139574-02
1243 Solaris/SunOS 5.10_x86 patch T139575-02
1244 -----
1245 6703683 Can't build VirtualBox on Build 88 or 89
1246 6737579 process_req_lib() in libld consumes file descriptors
1247 6685125 ld/elfdump do not handle ZERO terminator .eh_frame amd64 unwind entry
1248 -----
1249 All the above changes are incorporated in the following patches:

```

```

1250 Solaris/SunOS 5.10_sparc patch T139574-03
1251 Solaris/SunOS 5.10_x86 patch T139575-03
1252 -----
1253 -----
1254 -----
1255 Solaris 10 1009 (8th Q-update - s10u8)
1256 -----
1257 Bugid Risk Synopsis
1258 =====
1259 6782597 32-bit ld.so.1 needs to accept objects with large inode number
1260 6805502 The addition of "inline" keywords to sgs code broke the lint
1261 verification in S10
1262 6807864 ld.so.1 is susceptible to a fatal dlsym()/setlocale() race
1263 -----
1264 All the above changes are incorporated in the following patches:
1265 Solaris/SunOS 5.10_sparc patch T141692-01
1266 Solaris/SunOS 5.10_x86 patch T141693-01
1267 NOTE: The fix for 6805502 is only applicable to s10.
1268 -----
1269 6826410 ld needs to sort sections using 32-bit sort keys
1270 -----
1271 All the above changes are incorporated in the following patches:
1272 Solaris/SunOS 5.10_sparc patch T141771-01
1273 Solaris/SunOS 5.10_x86 patch T141772-01
1274 NOTE: The fix for 6826410 is also available for s9 in the following patches:
1275 Solaris/SunOS 5.9_sparc patch T112963-33
1276 Solaris/SunOS 5.9_x86 patch T113986-27
1277 -----
1278 6568447 bcp is broken by 6551627
1279 6599700 librtld_db needs better plugin support
1280 6713830 mdb dumped core reading a gcore
1281 6756048 rd_loadobj_iter() should always invoke brand plugin callback
1282 6786744 32-bit dbx failed with unknown rtld_db.so error on snv_104
1283 -----
1284 All the above changes are incorporated in the following patches:
1285 Solaris/SunOS 5.10_sparc patch T141444-06
1286 Solaris/SunOS 5.10_x86 patch T141445-06
1287 -----
1288 -----
1289 -----
1290 Solaris 10 1005 (9th Q-update - s10u9)
1291 -----
1292 Bugid Risk Synopsis
1293 =====
1294 6850124 dlopen reports "No such file or directory" in spite of ENOMEM
1295 when mmap fails in anon_map()
1296 6826513 ldd gets confused by a crle(1) LD_PRELOAD setting
1297 6684577 ld should propagate SHF_LINK_ORDER flag to ET_REL objects
1298 6524709 executables using /usr/lib/libc.so.1 as the ELF interpreter dump core
1299 (link-editor components only)
1300 -----
1301 All the above changes are incorporated in the following patches:
1302 Solaris/SunOS 5.10_sparc patch T143895-01
1303 Solaris/SunOS 5.10_x86 patch T143896-01
1304 -----
1305 -----
1306 -----
1307 Solaris 10 XXXX (10th Q-update - s10u10)
1308 -----
1309 Bugid Risk Synopsis
1310 =====
1311 6478684 isainfo/cpuid reports pause instruction not supported on amd64
1312 PSARC/2010/089 Removal of AV_386_PAUSE and AV_386_MON
1313 -----
1314 All the above changes are incorporated in the following patches:
1315 Solaris/SunOS 5.10_sparc patch TXXXXXX-XX

```

```

1316      Solaris/SunOS 5.10_x86      patch TXXXXXX-XX
1317 -----
1319 -----
1320 Solaris Nevada (OpenSolaris 2008.05, snv_86)
1321 -----
1322 Bugid      Risk Synopsis
1323 =====
1324 6409350 BrandZ project integration into Solaris (link-editor components only)
1325 6459189 UNIX03: *VSC* c99 compiler overwrites non-writable file
1326 6423746 add an option to relax the resolution of COMDAT relocations (D)
1327 4934427 runtime linker should load up static symbol names visible to
1328         dladdr() (D)
1329 PSARC/2006/526 SHT_SUNW_LDYNSSYM - default local symbol addition
1330 6448719 sys/elf.h could be updated with additional machine and ABI types
1331 6336605 link-editors need to support R_*_SIZE relocations
1332 PSARC/2006/558 R_*_SIZE relocation support
1333 6475375 symbol search optimization to reduce rescans
1334 6475497 elfdump(1) is misreporting sh_link
1335 6482058 lari(1) could be faster, and handle per-symbol filters better
1336 6482974 defining virtual address of text segment can result in an invalid data
1337         segment
1338 6476734 crle(1m) "-l" as described fails system, crle cores trying to fix
1339         /a/var/ld/ld.config in failsafe
1340 6487499 link_audit "make clobber" creates and populates proto area
1341 6488141 ld(1) should detect attempt to reference 0-length .bss section
1342 6496718 restricted visibility symbol references should trigger archive
1343         extraction
1344 6515970 HWCAP processing doesn't clean up fmap structure - browser fails to
1345         run java applet
1346 6494214 Refinements to symbolic binding, symbol declarations and
1347         interposition (D)
1348 PSARC/2006/714 ld(1) mapfile: symbol interpose definition
1349 6475344 DTrace needs ELF function and data symbols sorted by address (D)
1350 PSARC/2007/026 ELF symbol sort sections
1351 6518480 ld -melf_i386 doesn't complain (D)
1352 6519951 bfu is just another word for exit today (RPATH -> RUNPATH conversion
1353         bites us) (D)
1354 6521504 ld: hardware capabilities processing from relocatables objects needs
1355         hardening.
1356 6518322 Some ELF utilities need updating for .SUNW_ldynsym section (D)
1357 PSARC/2007/074 -L option for nm(1) to display SHT_SUNW_LDYNSSYM symbols
1358 6523787 dlopen() handle gets mistakenly orphaned - results in access to freed
1359         memory
1360 6531189 SEGV in dladdr()
1361 6527318 dlopen(name, RTLD_NOLOAD) returns handle for unloaded library
1362 6518359 extern mapfiles references to _init/_fini can create INIT/FINI
1363         addresses of 0
1364 6533587 ld.so.1: init/fini processing needs to compensate for interposer
1365         expectations
1366 6516118 Reserved space needed in ELF dynamic section and string table (D)
1367 PSARC/2007/127 Reserved space for editing ELF dynamic sections
1368 6535688 elfdump could be more robust in the face of Purify (D)
1369 6516665 The link-editors should be more resilient against gcc's symbol
1370         versioning
1371 6541004 hwcab filter processing can leak memory
1372 5108874 elfdump SEGVs on bad object file
1373 6547441 Uninitialized variable causes ld.so.1 to crash on object cleanup
1374 6341667 elfdump should check alignments of ELF header elements
1375 6387860 elfdump cores, when processing linux built ELF file
1376 6198202 mcs -d dumps core
1377 6246083 elfdump should allow section index specification
1378         (numeric -N equivalent) (D)
1379 PSARC/2007/247 Add -I option to elfdump
1380 6556563 elfdump section overlap checking is too slow for large files
1381 5006034 need ?E mapfile feature extension (D)

```

```

1382 6565476 rtdl symbol version check prevents GNU ld binary from running
1383 6567670 ld(1) symbol size/section size verification uncovers Haskell
1384         compiler inconsistency
1385 6530249 elfdump should handle ELF files with no section header table (D)
1386 PSARC/2007/395 Add -P option to elfdump
1387 6573641 ld.so.1 does not maintain parent relationship to a dlopen() caller.
1388 6577462 Additional improvements needed to handling of gcc's symbol versioning
1389 6583742 ELF string conversion library needs to lose static writable buffers
1390 6589819 ld generated reference to __tls_get_addr() fails when resolving to a
1391         shared object reference
1392 6595139 various applications should export yy* global variables for libl
1393 PSARC/2007/474 new ldd(1) -w option
1394 6597841 gelf_getdyn() reads one too many dynamic entries
1395 6603313 dlclosure() can fail to unload objects after fix for 6573641
1396 6234471 need a way to edit ELF objects (D)
1397 PSARC/2007/509 elfedit
1398 5035454 mixing -Kpic and -KPIC may cause SIGSEGV with -xarch=v9
1399 6473571 strip and mcs get confused and corrupt files when passed
1400         non-ELF arguments
1401 6253589 mcs has problems handling multiple SHT_NOTE sections
1402 6610591 do_reloc() should not require unused arguments
1403 6602451 new symbol visibilities required: EXPORTED, SINGLETON and ELIMINATE (D)
1404 PSARC/2007/559 new symbol visibilities - EXPORTED, SINGLETON, and
1405         ELIMINATE
1406 6570616 elfdump should display incorrectly aligned note section
1407 6614968 elfedit needs string table module (D)
1408 6620533 HWCAP filtering can leave uninitialized data behind - results in
1409         "rejected: Invalid argument"
1410 6617855 nodirect tag can be ignored when other syminfo tags are available
1411         (link-editor components only)
1412 6621066 Reduce need for new elfdump options with every section type (D)
1413 PSARC/2007/620 elfdump -T, and simplified matching
1414 6627765 soffice failure after integration of 6603313 - dangling GROUP pointer.
1415 6319025 SUNWbtool packaging issues in Nevada and S10u1.
1416 6626135 elfedit capabilities str->value mapping should come from
1417         usr/src/common/elfcap
1418 6642769 ld(1) -z combrelloc should become default behavior (D)
1419 PSARC/2008/006 make ld(1) -z combrelloc become default behavior
1420 6634436 XFFLAG should be updated. (link-editor components only)
1421 6492726 Merge SHF_MERGE|SHF_STRINGS input sections (D)
1422 4947191 OSNet should use direct bindings (link-editor components only)
1423 6654381 lazy loading fall-back needs optimizing
1424 6658385 ld core dumps when building Xorg on nv_82
1425 6516808 ld.so.1's token expansion provides no escape for platforms that don't
1426         report HWCAP
1427 6668534 Direct bindings can compromise function address comparisons from
1428         executables
1429 6667661 Direct bindings can compromise executables with insufficient copy
1430         relocation information
1431 6357282 ldd should recognize PARENT and EXTERN symbols (D)
1432 PSARC/2008/148 new ldd(1) -p option
1433 6672394 ldd(1) unused dependency processing is tricked by relocations errors
1434 -----
1436 -----
1437 Solaris Nevada (OpenSolaris 2008.11, snv_101)
1438 -----
1439 Bugid      Risk Synopsis
1440 =====
1441 6671255 link-editor should support cross linking (D)
1442 PSARC/2008/179 cross link-editor
1443 6674666 elfedit dyn:posflag1 needs option to locate element via NEEDED item
1444 6675591 elfwrap - wrap data in an ELF file (D,P)
1445 PSARC/2008/198 elfwrap - wrap data in an ELF file
1446 6678244 elfdump dynamic section sanity checking needs refinement
1447 6679212 sgs use of SCCS id for versioning is obstacle to mercurial migration

```

```

1448 6681761 lies, darn lies, and linker README files
1449 6509323 Need to disable the Multiple Files loading - same name, different
1450 directories (or its stat() use)
1451 6686889 ld.so.1 regression - bad pointer created with 6509323 integration
1452 6695681 ldd(1) crashes when run from a chrooted environment
1453 6516212 usr/src/cmd/sgs/libelf warlock targets should be fixed or abandoned
1454 6678310 using LD_AUDIT, ld.so.1 calls shared library's .init before library is
1455 fully relocated (link-editor components only)
1456 6699594 The ld command has a problem handling 'protected' mapfile keyword.
1457 6699131 elfdump should display core file notes (D)
1458 6702260 single threading .init/.fini sections breaks staroffice
1459 6703919 boot hangs intermittently on x86 with onnv daily.0430 and on
1460 6701798 ld can enter infinite loop processing bad mapfile
1461 6706401 direct binding copy relocation fallback is insufficient for ild
1462 generated objects
1463 6705846 multithreaded C++ application seems to get deadlocked in the dynamic
1464 linker code
1465 6686343 ldd(1) - unused search path diagnosis should be enabled
1466 6712292 ld.so.1 should fall back to an interposer for failed direct bindings
1467 6716350 usr/src/cmd/sgs should be linted by nightly builds
1468 6720509 usr/src/cmd/sgs/sgsdemangler should be removed
1469 6617475 gas creates erroneous FILE symbols [was: ld.so.1 is reported as
1470 false positive by wsdiff]
1471 6724311 dldump() mishandles R_AMD64_JUMP_SLOT relocations
1472 6724774 elfdump -n doesn't print siginfo structure
1473 6728555 Fix for amd64 aw (6617475) breaks pure gcc builds
1474 6734598 ld(1) archive processing failure due to mismatched file descriptors (D)
1475 6735939 ld(1) discarded symbol relocations errors (Studio and GNU).
1476 6354160 Solaris linker includes more than one copy of code in binary when
1477 linking gnu object code
1478 6744003 ld(1) could provide better argument processing diagnostics (D)
1479 PSARC 2008/583 add gld options to ld(1)
1480 6749055 ld should generate GNU style VERSYM indexes for VERNEED records (D)
1481 PSARC/2008/603 ELF objects to adopt GNU-style Versym indexes
1482 6752728 link-editor can enter UNDEF symbols in symbol sort sections
1483 6756472 AOUT search path pruning (D)
1484 -----
1486 -----
1487 Solaris Nevada (OpenSolaris 2009.06, snv_111)
1488 -----
1489 Bugid Risk Synopsis
1490 =====
1492 6754965 introduce the SF1_SUNW_ADDR32 bit in software capabilities (D)
1493 (link-editor components only)
1494 PSARC/2008/622 32-bit Address Restriction Software Capabilities Flag
1495 6756953 customer requests that DT_CONFIG strings be honored for secure apps (D)
1496 6765299 ld --version-script option not compatible with GNU ld (D)
1497 6748160 problem with -zrescan (D)
1498 PSARC/2008/651 New ld archive rescan options
1499 6763342 sloppy relocations need to get sloppier
1500 6736890 PT_SUNWBSS should be disabled (D)
1501 PSARC/2008/715 PT_SUNWBSS removal
1502 6772661 ldd/lddstub/ld.so.1 dump core in current nightly while processing
1503 libsoftcrypto-hwcap.so.1
1504 6765931 mcs generates unlink(NULL) system calls
1505 6775062 remove /usr/lib/libldstab.so (D)
1506 6782977 ld segfaults after support lib version error sends bad args to vprintf()
1507 6773695 ld -z nopartial can break non-pic objects
1508 6778453 RTLD_GROUP prevents use of application defined malloc
1509 6789925 64-bit applications with SF1_SUNW_ADDR32 require non-default starting
1510 address
1511 6792906 ld -z nopartial fix breaks TLS
1512 6686372 ld.so.1 should use mmapobj(2)
1513 6726108 dlopen() performance could be improved.

```

```

1514 6792836 ld is slow when processing GNU linkonce sections
1515 6797468 ld.so.1: orphaned handles aren't processed correctly
1516 6798676 ld.so.1: enters infinite loop with realloc/defragmentation logic
1517 6237063 request extension to dl* family to provide segment bounds
1518 information (D)
1519 PSARC/2009/054 dlinfo(3c) - segment mapping retrieval
1520 6800388 shstrtab can be sized incorrectly when -z ignore is used
1521 6805009 ld.so.1: link map control list tear down leaves dangling pointer -
1522 pfinstall does it again.
1523 6807050 GNU linkonce sections can create duplicate and incompatible
1524 eh_frame FDE entries
1525 -----
1527 -----
1528 Solaris Nevada
1529 -----
1530 Bugid Risk Synopsis
1531 =====
1532 6813909 generalize eh_frame support to non-amd64 platforms
1533 6801536 ld: mapfile processing oddities unveiled through mmapobj(2) observations
1534 6802452 libelf shouldn't use MS_SYNC
1535 6818012 nm tries to modify readonly segment and dumps core
1536 6821646 xVM dom0 doesn't boot on daily.0324 and beyond
1537 6822828 librtld_db can return RD_ERR before RD_NOMAPS, which compromises dbx
1538 expectations.
1539 6821619 Solaris linkers need systematic approach to ELF OSABI (D)
1540 PSARC/2009/196 ELF objects to set OSABI / elfdump -O option
1541 6827468 6801536 breaks 'ld -s' if there are weak/strong symbol pairs
1542 6715578 AOUT (BCP) symbol lookup can be compromised with lazy loading.
1543 6752883 ld.so.1 error message should be buffered (not sent to stderr).
1544 6577982 ld.so.1 calls getpid() before it should when any LD_* are set
1545 6831285 linker LD_DEBUG support needs improvements (D)
1546 6806791 filter builds could be optimized (link-editor components only)
1547 6823371 calloc() uses suboptimal memset() causing 15% regression in SpecCPU2006
1548 gcc code (link-editor components only)
1549 6831308 ld.so.1: symbol rescanning does a little too much work
1550 6837777 ld ordered section code uses too much memory and works too hard
1551 6841199 Undo 10 year old workaround and use 64-bit ld on 32-bit objects
1552 6784790 ld should examine archives to determine output object class/machine (D)
1553 PSARC/2009/305 ld -32 option
1554 6849998 remove undocumented mapfile $SPECVERS and $NEED options
1555 6851224 elf_getshnum() and elf_getshstrndx() incompatible with 2002 ELF gABI
1556 agreement (D)
1557 PSARC/2009/363 replace elf_getphnum, elf_getshnum, and elf_getshstrndx
1558 6853809 ld.so.1: rescan fallback optimization is invalid
1559 6854158 ld.so.1: interposition can be skipped because of incorrect
1560 caller/destination validation
1561 6862967 rd_loadobj_iter() failing for core files
1562 6856173 streams core dumps when compiled in 64bit with a very large static
1563 array size
1564 6834197 ld pukes when given an empty plate
1565 6516644 per-symbol filtering shouldn't be allowed in executables
1566 6878605 ld should accept '%' syntax when matching input SHT_PROGBITS sections
1567 6850768 ld option to autogenerate wrappers/interposers similar to GNU ld
1568 --wrap (D)
1569 PSARC/2009/493 ld -z wrap option
1570 6888489 Null environment variables are not overriding crle(1) replaceable
1571 environment variables.
1572 6885456 Need to implement GNU-ld behavior in construction of .init/.fini
1573 sections
1574 6900241 ld should track SHT_GROUP sections by symbol name, not section name
1575 6901773 Special handling of STT_SECTION group signature symbol for GNU objects
1576 6901895 Failing asserts in ld update_osym() trying to build gcc 4.5 development
1577 head
1578 6909523 core dump when run "LD_DEBUG=help ls" in non-English locale
1579 6903688 mdb(1) can't resolve certain symbols in solaris10-branded processes

```

```

1580      from the global zone
1581 6923449 elfdump misinterprets _init/_fini symbols in dynamic section test
1582 6914728 Add dl_iterate_phdr() function to ld.so.1 (D)
1583      PSARC/2010/015 dl_iterate_phdr
1584 6916788 ld version 2 mapfile syntax (D)
1585      PSARC/2009/688 Human readable and extensible ld mapfile syntax
1586 6929607 ld generates incorrect VERDEF entries for ET_REL output objects
1587 6924224 linker should ignore SUNW_dof when calculating the elf checksum
1588 6918143 symbol capabilities (D)
1589      PSARC/2010/022 Linker-editors: Symbol Capabilities
1590 6910387 .tdata and .tbss separation invalidates TLS program header information
1591 6934123 elfdump -d core dumps on PA-RISC elf
1592 6931044 ld should not allow SHT_PROGBITS .eh_frame sections on amd64 (D)
1593 6931056 pvs -r output can include empty versions in output
1594 6938628 ld.so.1 should produce diagnostics for all dl*() entry points
1595 6938111 nm 'No symbol table data' message goes to stdout
1596 6941727 ld relocation cache memory use is excessive
1597 6932220 ld -z allextact skips objects that lack global symbols
1598 6943772 Testing for a symbols existence with RTLD_PROBE is compromised by
1599      RTLD_BIND_NOW
1600      PSARC/2010/XXX Deferred symbol references
1601 6943432 dlsym(RTLD_PROBE) should only bind to symbol definitions
1602 6668759 an external method for determining whether an ELF dependency is optional
1603 6954032 Support library with ld_open and -z allextact in snv_139 do not mix
1604 6949596 wrong section alignment generated in joint compilation with shared
1605      library
1606 6961755 ld.so.1's -e arguments should take precedence over environment
1607      variables. (D)
1608 6748925 moe returns wrong hwcap library in some circumstances
1609 6916796 OSnet mapfiles should use version 2 link-editor syntax
1610 6964517 OSnet mapfiles should use version 2 link-editor syntax (2nd pass)
1611 6948720 SHT_INIT_ARRAY etc. section names don't follow ELF gABI (D)
1612 6962343 sgsmgs should use mkstemp() for temporary file creation
1613 6965723 libsoftcrypto symbol capabilities rely on compiler generated
1614      capabilities - gcc failure (link-editor components only)
1615 6952219 ld support for archives larger than 2 GB (D, P)
1616      PSARC/2010/224 Support for archives larger than 2 GB
1617 6956152 dlclose() from an auditor can be fatal. Preinit/activity events should
1618      be more flexible. (D)
1619 6971440 moe can core dump while processing libc.
1620 6972234 sgs demo's could use some cleanup
1621 6935867 .dynamic could be readonly in sharable objects
1622 6975290 ld mishandles GOT relocation against local ABS symbol
1623 6972860 ld should provide user guidance to improve objects (D)
1624      PSARC/2010/312 Link-editor guidance
1625 -----

```

```

1627 -----
1628 Illumos
1629 -----
1630 Bugid   Risk Synopsis
1631 =====

```

```

1633 308      ld may misalign sections only preceded by empty sections
1634 1301      ld crashes with '-z ignore' due to a null data descriptor
1635 1626      libld may accidentally return success while failing
1636 2413      %ymm* need to be preserved on way through PLT
1637 3210      ld should tolerate SHT_PROGBITS for .eh_frame sections on amd64
1638 3228      Want -zassert-deflib for ld
1639 3230      ld.so.1 should check default paths for DT_DEPAUDIT
1640 3260      linker is insufficiently careful with strtok
1641 3261      linker should ignore unknown hardware capabilities
1642 3265      link-editor builds bogus .eh_frame_hdr on ia32
1643 3453      GNU comdat redirection does exactly the wrong thing
1644 3439      discarded sections shouldn't end up on output lists
1645 3436      relocatable objects also need sloppy relocation

```

```

1646 3451      archive libraries with no symbols shouldn't require a string table
1647 3616      SHF_GROUP sections should not be discarded via other COMDAT mechanisms
1648 3709      need sloppy relocation for GNU .debug_macro
1649 3722      link-editor is over restrictive of R_AMD64_32 addends
1650 3926      multiple extern map file definitions corrupt symbol table entry
1651 3999      libld extended section handling is broken
1652 4003      didump() can't deal with extended sections
1653 4227      ld --library-path is translated to -l-path, not -L
1654 4270      ld(1) argument error reporting is still pretty bad
1655 4383      libelf can't write extended sections when ELF_F_LAYOUT
1656 4959      completely discarded merged string sections will corrupt output objects
1657 4996      rtdld_init race leads to incorrect symbol values
1658 5688      ELF tools need to be more careful with dwarf data
1659 6098      ld(1) should not require symbols which identify group sections be global
1660 6252      ld should merge function/data-sections in the same manner as GNU ld
1661 7323      ld(1) -zignore can erroneously discard init and fini arrays as unreferen
1662 7594      ld -zaslr should accept Solaris-compatible values
1663 8616      ld has trouble parsing -z options specified with -wl
1664 10267      ld and GCC disagree about i386 local dynamic TLS
1665 #endif /* ! codereview */

```