```
**********************************************************
   46096 Thu Feb 28 22:40:42 2019
new/usr/src/cmd/sgs/libld/common/machrel.amd.c
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
**********************************************************
______unchanged_portion_omitted_

 517 #define REX_B           0x1
 518 #define REX_X           0x2
 519 #define REX_R           0x4
 520 #define REX_W           0x8
 521 #define REX_PREFIX      0x40

 523 #define REX_RW          (REX_PREFIX | REX_R | REX_W)
 524 #define REX_BW          (REX_PREFIX | REX_B | REX_W)
 525 #define REX_BRW         (REX_PREFIX | REX_B | REX_R | REX_W)

 527 #define REG_ESP         0x4

 529 #define INSN_ADDMR      0x03    /* addq mem,reg */
 530 #define INSN_ADDIR      0x81    /* addq imm,reg */
 531 #define INSN_MOVMR      0x8b    /* movq mem,reg */
 532 #define INSN_MOVIR      0xc7    /* movq imm,reg */
 533 #define INSN_LEA        0x8d    /* leaq mem,reg */

 535 static Fixupret
 536 tls_fixups(Ofl_desc *ofl, Rel_desc *arsp)
 537 {
 538         Sym_desc        *sdp = arsp->rel_sym;
 539         Word            rtype = arsp->rel_rtype;
 540         uchar_t         *offset;

 542         offset = (uchar_t *)((uintptr_t)arsp->rel_roffset +
 543             (uintptr_t)_elf_getxoff(arsp->rel_isdesc->is_indata) +
 544             (uintptr_t)RELAUX_GET_OSDESC(arsp)->os_outdata->d_buf);

 546         /*
 547          * Note that in certain of the original insn sequences below, the
 548          * instructions are not necessarily adjacent
 549          */
 550         if (sdp->sd_ref == REF_DYN_NEED) {
 551                 /*
 552                  * IE reference model
 553                  */
 554                 switch (rtype) {
 555                 case R_AMD64_TLSGD:
 556                         /*
 557                          *  GD -> IE
 558                          *
 559                          * Transition:
 560                          *      0x00 .byte 0x66
 561                          *      0x01 leaq x@tlsgd(%rip), %rdi
 562                          *      0x08 .word 0x6666
 563                          *      0x0a rex64
 564                          *      0x0b call __tls_get_addr@plt
 565                          *      0x10
 566                          * To:
 567                          *      0x00 movq %fs:0, %rax
 568                          *      0x09 addq x@gottpoff(%rip), %rax
 569                          *      0x10
 570                          */
 571                         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
 572                             R_AMD64_GOTTPOFF, arsp, ld_reloc_sym_name));
 573                         arsp->rel_rtype = R_AMD64_GOTTPOFF;
 574                         arsp->rel_roffset += 8;
 575                         arsp->rel_raddend = (Sxword)-4;
```



```
 577                         /*
 578                          * Adjust 'offset' to beginning of instruction
 579                          * sequence.
 580                          */
 581                         offset -= 4;
 582                         (void) memcpy(offset, tlsinstr_gd_ie,
 583                             sizeof (tlsinstr_gd_ie));
 584                         return (FIX_RELOC);

 586                 case R_AMD64_PLT32:
 587                         /*
 588                          * Fixup done via the TLS_GD relocation.
 589                          */
 590                         DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
 591                             R_AMD64_NONE, arsp, ld_reloc_sym_name));
 592                         return (FIX_DONE);
 593                 }
 594         }

 596         /*
 597          * LE reference model
 598          */
 599         switch (rtype) {
 600         case R_AMD64_TLSGD:
 601                 /*
 602                  * GD -> LE
 603                  *
 604                  * Transition:
 605                  *      0x00 .byte 0x66
 606                  *      0x01 leaq x@tlsgd(%rip), %rdi
 607                  *      0x08 .word 0x6666
 608                  *      0x0a rex64
 609                  *      0x0b call __tls_get_addr@plt
 610                  *      0x10
 611                  * To:
 612                  *      0x00 movq %fs:0, %rax
 613                  *      0x09 leaq x@tpoff(%rax), %rax
 614                  *      0x10
 615                  */
 616                 DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
 617                     R_AMD64_TPOFF32, arsp, ld_reloc_sym_name));
 618                 arsp->rel_rtype = R_AMD64_TPOFF32;
 619                 arsp->rel_roffset += 8;
 620                 arsp->rel_raddend = 0;

 622                 /*
 623                  * Adjust 'offset' to beginning of instruction sequence.
 624                  */
 625                 offset -= 4;
 626                 (void) memcpy(offset, tlsinstr_gd_le, sizeof (tlsinstr_gd_le));
 627                 return (FIX_RELOC);

 629         case R_AMD64_GOTTPOFF: {
 630                 /*
 631                  * IE -> LE
 632                  *
 633                  * Transition 1:
 634                  *      movq %fs:0, %reg
 635                  *      addq x@gottpoff(%rip), %reg
 636                  * To:
 637                  *      movq %fs:0, %reg
 638                  *      leaq x@tpoff(%reg), %reg
 639                  *
 640                  * Transition (as a special case):
 641                  *      movq %fs:0, %r12/%rsp
```

```
642                  *      addq x@gottpoff(%rip), %r12/%rsp
643                  * To:
644                  *      movq %fs:0, %r12/%rsp
645                  *      addq x@tpoff(%rax), %r12/%rsp
646                  *
647                  * Transition 2:
648                  *      movq x@gottpoff(%rip), %reg
649                  *      movq %fs:(%reg), %reg
650                  * To:
651                  *      movq x@tpoff(%reg), %reg
652                  *      movq %fs:(%reg), %reg
653                  */
654                 Conv_inv_buf_t  inv_buf;
655                 uint8_t reg;            /* Register */

657                 offset -= 3;

659                 reg = offset[2] >> 3; /* Encoded dest. reg. operand */

661                 DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
662                     R_AMD64_TPOFF32, arsp, ld_reloc_sym_name));
663                 arsp->rel_rtype = R_AMD64_TPOFF32;
664                 arsp->rel_raddend = 0;

666                 /*
667                  * This is transition 2, and the special case of form 1 where
668                  * a normal transition would index %rsp or %r12 and need a SIB
669                  * byte in the leaq for which we lack space
670                  */
671                 if ((offset[1] == INSN_MOVMR) ||
672                     ((offset[1] == INSN_ADDMR) && (reg == REG_ESP))) {
673                         /*
674                          * If we needed an extra bit of MOD.reg to refer to
675                          * this register as the dest of the original movq we
676                          * need an extra bit of MOD.rm to refer to it in the
677                          * dest of the replacement movq or addq.
678                          */
679                         if (offset[0] == REX_RW)
680                                 offset[0] = REX_BW;

682                         offset[1] = (offset[1] == INSN_MOVMR) ?
683                             INSN_MOVIR : INSN_ADDIR;
684                         offset[2] = 0xc0 | reg;

686                         return (FIX_RELOC);
687                 } else if (offset[1] == INSN_ADDMR) {
688                         /*
689                          * If we needed an extra bit of MOD.reg to refer to
690                          * this register in the dest of the addq we need an
691                          * extra bit of both MOD.reg and MOD.rm to refer to it
692                          * in the source and dest of the leaq
693                          */
694                         if (offset[0] == REX_RW)
695                                 offset[0] = REX_BRW;

697                         offset[1] = INSN_LEA;
698                         offset[2] = 0x80 | (reg << 3) | reg;

700                         return (FIX_RELOC);
701                 }

703                 ld_eprintf(ofl, ERR_FATAL, MSG_INTL(MSG_REL_BADTLSINS),
704                     conv_reloc_amd64_type(arsp->rel_rtype, 0, &inv_buf),
705                     arsp->rel_isdesc->is_file->ifl_name,
706                     ld_reloc_sym_name(arsp),
707                     arsp->rel_isdesc->is_name,
```



```
708                         EC_OFF(arsp->rel_roffset));
709                 return (FIX_ERROR);
710         }
711         case R_AMD64_TLSLD:
712                 /*
713                  * LD -> LE
714                  *
715                  * Transition
716                  *      0x00 leaq x1@tlsgd(%rip), %rdi
717                  *      0x07 call __tls_get_addr@plt
718                  *      0x0c
719                  * To:
720                  *      0x00 .byte 0x66
721                  *      0x01 .byte 0x66
722                  *      0x02 .byte 0x66
723                  *      0x03 movq %fs:0, %rax
724                  */
725                 DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
726                     R_AMD64_NONE, arsp, ld_reloc_sym_name));
727                 offset -= 3;
728                 (void) memcpy(offset, tlsinstr_ld_le, sizeof (tlsinstr_ld_le));
729                 return (FIX_DONE);

731         case R_AMD64_DTPOFF32:
732                 /*
733                  * LD->LE
734                  *
735                  * Transition:
736                  *      0x00 leaq x1@dtpoff(%rax), %rcx
737                  * To:
738                  *      0x00 leaq x1@tpoff(%rax), %rcx
739                  */
740                 DBG_CALL(Dbg_reloc_transition(ofl->ofl_lml, M_MACH,
741                     R_AMD64_TPOFF32, arsp, ld_reloc_sym_name));
742                 arsp->rel_rtype = R_AMD64_TPOFF32;
743                 arsp->rel_raddend = 0;
743                 return (FIX_RELOC);
744         }

746         return (FIX_RELOC);
747 }
```

_____unchanged_portion_omitted_

```
**********************************************************
   88745 Thu Feb 28 22:40:43 2019
new/usr/src/cmd/sgs/packages/common/SUNWonld-README
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
**********************************************************
```

```
#
# Copyright (c) 1996, 2010, Oracle and/or its affiliates. All rights reserved.
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
# Note: The contents of this file are used to determine the versioning
#       information for the SGS toolset. The number of CRs listed in
#       this file must grow monotonically, or the SGS version will
#       move backwards, causing a great deal of confusion. As such,
#       CRs must never be removed from this file. See
#       libconv/common/bld_vernote.ksh, and bug#4519569 for more
#       details on SGS versioning.
#
--------------------------------------------------------------------------------
SUNWonld - link-editors development package.
--------------------------------------------------------------------------------

  The SUNWonld package is an internal development package containing the
  link-editors and some related tools.  All components live in the OSNET
  source base, but not all components are delivered as part of the normal
  OSNET consolidation.  The intent of this package is to provide access
  to new features/bugfixes before they become generally available.

  General link-editor information can be found:

    http://linkers.central/
    http://linkers.sfbay/       (also known as linkers.eng)

  Comments and Questions:

    Contact Rod Evans, Ali Bahrami, and/or Seizo Sakurai.

  Warnings:

    The postremove script for this package employs /usr/sbin/static/mv,
    and thus, besides the common core dependencies, this package also
    has a dependency on the SUNWsutl package.

  Patches:

    If the patch has been made official, you'll find it in:

        http://sunsolve.east/cgi/show.pl?target=patches/os-patches
```



```
    If it hasn't been released, the patch will be in:

        /net/sunsoftpatch/patches/temporary

    Note, any patches logged here refer to the temporary ("T") name, as we
    never know when they're made official, and although we try to keep all
    patch information up-to-date the real status of any patch can be
    determined from:

        http://sunsoftpatch.eng

    If it has been obsoleted, the patch will be in:

        /net/on${RELEASE}-patch/on${RELEASE}/patches/${MACH}/obsolete


  History:

    Note, starting after Solaris 10, letter codes in parenthesis may
    be found following the bug synopsis. Their meanings are as follows:

        (D) A documentation change accompanies the implementation change.
        (P) A packaging change accompanies the implementation change.

    In all cases, see the implementation bug report for details.

    The following bug fixes exist in the OSNET consolidation workspace
    from which this package is created:

---------
Solaris 8
---------
Bugid   Risk Synopsis
================================================================================
4225937 i386 linker emits sparc specific warning messages
4215164 shf_order flag handling broken by fix for 4194028.
4215587 using ld and the -r option on solaris 7 with compiler option -xarch=v9
        causes link errors.
4234657 103627-08 breaks purify 4.2 (plt padding should not be enabled for
        32-bit)
4235241 dbx no longer gets dlclose notification.
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.7_sparc         patch 106950-05  (never released)
        Solaris/SunOS 5.7_x86           patch 106951-05  (never released)
        Solaris/SunOS 5.6_sparc         patch 107733-02  (never released)
        Solaris/SunOS 5.6_x86           patch 107734-02
--------------------------------------------------------------------------------
4248290 inetd dumps core upon bootup - failure in dlclose() logic.
4238071 dlopen() leaks while descriptors under low memory conditions
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.7_sparc         patch 106950-06
        Solaris/SunOS 5.7_x86           patch 106951-06
        Solaris/SunOS 5.6_sparc         patch 107733-03  (never released)
        Solaris/SunOS 5.6_x86           patch 107734-03
--------------------------------------------------------------------------------
4267980 INITFIRST flag of the shard object could be ignored.
--------------------------------------------------------------------------------
All the above changes plus:
    4238973 fix for 4121152 affects linking of Ada objects
    4158744 patch 103627-02 causes core when RPATH has blank entry and
            dlopen/dlclose is used
are incorporated in the following patches:
        Solaris/SunOS 5.5.1_sparc       patch 103627-12  (never released)
        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 xxxxxxx 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 sgsmsg 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 rtld 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
```

```
4355795 ldd -r now gives "displacement relocated" warnings
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.7_sparc         patch 106950-13
        Solaris/SunOS 5.7_x86           patch 106951-13
        Solaris/SunOS 5.6_sparc         patch 107733-09
        Solaris/SunOS 5.6_x86           patch 107734-09
--------------------------------------------------------------------------------
4210412 versioning a static executable causes ld to core dump
4219652 Linker gives misleading error about not finding main (xarch=v9)
4103449 ld command needs a command line flag to force 64-bits
4187211 problem with RDISP32 linking in copy-relocated objects
4287274 dladdr, dlinfo do not provide the full path name of a shared object
4297563 dlclose still does not remove all objects.
4250694 rtld_db needs a new auxvec entry
4235315 new features for rtld_db (DT_CHECKSUM, dynamic linked .o files
4303609 64bit libelf.so.1 does not properly implement elf_hash()
4310901 su.static fails when OSNet build with lazy-loading
4310324 elf_errno() causes Bus Error(coredump) in 64-bit multithreaded programs
4306415 ld core dump
4316531 BCP: possible failure with dlclose/_preexec_exit_handlers
4313765 LD_BREADTH should be shot
4318162 crle uses automatic strings in putenv.
4255943 Description of -t option incomplete.
4322528 sgs message test infrastucture needs improvement
4239213 Want an API to obtain linker's search path
4324134 use of extern mapfile directives can contribute unused symbols
4322581 ELF data structures could be layed out more efficiently...
4040628 Unnecessary section header symbols should be removed from .dynsym
4300018 rtld: bindlock should be freed before calling call_fini()
4336102 dlclose with non-deletable objects can mishandle dependencies
4329785 mixing of SHT_SUNW_COMDAT & SHF_ORDERED causes ld to seg fault
4334617 COPY relocations should be produces for references to .bss symbols
4248250 relcoation of local ABS symbols incorrect
4335801 For complimentary alignments eliminate ld: warning: symbol `ll'
        has differing a
4336980 ld.so.1 relative path processing revisited
4243097 dlerror(3DL) is not affected by setlocale(3C).
4344528 dump should remove -D and -l usage message
xxxxxxx enable LD_ALTEXEC to access alternate link-editor
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-06
        Solaris/SunOS 5.8_x86           patch 109148-06
--------------------------------------------------------------------------------

-----------------------------------
Solaris 8 101 (3rd Q-update - s28u3)
-----------------------------------
Bugid   Risk Synopsis
================================================================================
4346144 link-auditing: plt_tracing fails if LA_SYMB_NOPLTENTER given after
        being bound
4346001 The ld should support mapfile syntax to generate PT_SUNWSTACK segment
4349137 rtld_db: A third fallback method for locating the linkmap
4343417 dladdr interface information inadequate
4343801 RFE: crle(1): provide option for updating configuration files
4346615 ld.so.1 attempting to open a directory gives: No such device
4352233 crle should not honor umask
4352330 LD_PRELOAD cannot use absolute path for privileged program
4357805 RFE: man page for ld(1) does not document all -z or -B options in
        Solaris 8 9/00
4358751 ld.so.1: LD_XXX environ variables and LD_FLAGS should be synchronized.
4358862 link editors should reference "64" symlinks instead of sparcv9 (ia64).
4356879 PLTs could use faster code sequences in some cases
4367118 new fast baplt's fail when traversed twice in threaded application
```



```
4366905 Need a way to determine path to a shared library
4351197 nfs performance problem by 103627-13
4367405 LD_LIBRARY_PATH_64 not being used
4354500 SHF_ORDERED ordered scections does not properly sort sections
4369068 ld(1)'s weak symbol processing is inefficient (slow and doesn't scale).
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-07
        Solaris/SunOS 5.8_x86           patch 109148-07
        Solaris/SunOS 5.7_sparc         patch 106950-14
        Solaris/SunOS 5.7_x86           patch 106951-14
--------------------------------------------------------------------------------

-----------------------------------
Solaris 8 701 (5th Q-update - s28u5)
-----------------------------------
Bugid   Risk Synopsis
================================================================================
4368846 ld(1) fails to version some interfaces given in a mapfile
4077245 dump core dump on null pointer.
4372554 elfdump should demangle symbols (like nm, dump)
4371114 dlclose may unmap a promiscuous object while it's still in use.
4204447 elfdump should understand SHN_AFTER/SHN_BEGIN macro
4377941 initialization of interposers may not occur
4381116 ldd/ld.so.1 could aid in detecting unused dependencies
4381783 dlopen/dlclose of a libCrun+libthread can dump core
4385402 linker & run-time linker must support gABI ELF updates
4394698 ld.so.1 does not process DF_SYMBOLIC - not gABI conforming
4394212 the link editor quietly ignores missing support libraries
4390308 ld.so.1 should provide more flexibility LD_PRELOAD'ing 32-bit/64-bit
        objects
4401232 crle(1) could provide better flexibility for alternatives
4401815 fix misc nits in debugging output...
4402861 cleanup /usr/demo/link_audit & /usr/tmp/librtld_db demo source code...
4393044 elfdump should allow raw dumping of sections
4413168 SHF_ORDERED bit causes linker to generate a separate section
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-08
        Solaris/SunOS 5.8_x86           patch 109148-08
--------------------------------------------------------------------------------
4452202 Typos in <sys/link.h>
4452220 dump doesn't support RUNPATH
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-09
        Solaris/SunOS 5.8_x86           patch 109148-09
--------------------------------------------------------------------------------

-----------------------------------
Solaris 8 1001 (6th Q-update - s28u6)
-----------------------------------
Bugid   Risk Synopsis
================================================================================
4421842 fixups in SHT_GROUP processing required...
4450433 problem with liblddbg output on -Dsection,detail when
        processing SHF_LINK_ORDER
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-10
        Solaris/SunOS 5.8_x86           patch 109148-10
        Solaris/SunOS 5.7_sparc         patch 106950-15
        Solaris/SunOS 5.7_x86           patch 106951-15
--------------------------------------------------------------------------------
4463473 pldd showing wrong output
--------------------------------------------------------------------------------
```

```
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-11
        Solaris/SunOS 5.8_x86           patch 109148-11
-------------------------------------------------------------------------------

-----------------------------------
Solaris 8 202 (7th Q-update - s28u7)
-----------------------------------
Bugid   Risk Synopsis
===============================================================================
4488954 ld.so.1 reuses same buffer to send ummapping range to
        _preexec_exit_handlers()
-------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-12
        Solaris/SunOS 5.8_x86           patch 109148-12
-------------------------------------------------------------------------------

---------
Solaris 9
---------
Bugid   Risk Synopsis
===============================================================================
4505289 incorrect handling of _START_ and _END_
4506164 mcs does not recognize #linkbefore or #linkafter qualifiers
4447560 strip is creating unexecutable files...
4513842 library names not in ld.so string pool cause corefile bugs
-------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-13
        Solaris/SunOS 5.8_x86           patch 109148-13
        Solaris/SunOS 5.7_sparc         patch 106950-16
        Solaris/SunOS 5.7_x86           patch 106951-16
-------------------------------------------------------------------------------
4291384 ld -M with a mapfile does not properly align Fortran REAL*8 data
4413322 SunOS 5.9 librtld_db doesn't show dlopened ".o" files anymore?
4429371 librtld_db busted on ia32 with SC6.x compilers...
4418274 elfdump dumps core on invalid input
4432224 libelf xlate routines are out of date
4433643 Memory leak using dlopen()/dlclose() in Solaris 8
4446564 ldd/lddstub - core dump conditions
4446115 translating SUNW_move sections is broken
4450225 The rdb command can fall into an infinite loop
4448531 Linker Causes Segmentation Fault
4453241 Regression in 4291384 can result in empty symbol table.
4453398 invalid runpath token can cause ld to spin.
4460230 ld (for OS 5.8 and 5.9) loses error message
4462245 ld.so.1 core dumps when executed directly...
4455802 need more flexibility in establishing a support library for ld
4467068 dyn_plt_entsize not properly initialized in ld.so.1
4468779 elf_plt_trace_write() broken on i386 (link-auditing)
4465871 -zld32 and -zld64 does not work the way it should
4461890 bad shared object created with -zredlocsym
4469400 ld.so.1: is_so_loaded isn't as efficient as we thought...
4469566 lazy loading fallback can reference un-relocated objects
4470493 libelf incorectly translates NOTE sections accross architectures...
4469684 rtld leaks dl_handles and permits on dlopen/dlclose
4475174 ld.so.1 prematurly reports the failure to load a object...
4475514 ld.so.1 can core dump in memory allocation fails (no swap)
4481851 Setting ld.so.1 environment variables globally would be useful
4482035 setting LD_PROFILE & LD_AUDIT causes ping command to issue warnings
        on 5.8
4377735 segment reservations cause sbrk() to fail
4491434 ld.so.1 can leak file-descriptors when loading same named objects
4289232 some of warning/error/debugging messages from libld.so can be revised
4462748 Linker Portion of TLS Support
```



```
4496718 run-time linkers mutex_locks not working with ld_libc interface
4497270 The -zredlocsym option should not eliminate partially initialized local
        symbols
4496963 dumping an object with crle(1) that uses $ORIGIN can loose its
        dependencies
4499413 Sun linker orders of magnitude slower than gnu linker
4461760 lazy loading libXm and libXt can fail.
4469031 The partial initialized (local) symbols for intel platform is not
        working.
4492883 Add link-editor option to multi-pass archives to resolve unsatisfied
        symbols
4503731 linker-related commands misspell "argument"
4503768 whocalls(1) should output messages to stderr, not stdout
4503748 whocalls(1) usage message and manpage could be improved
4503625 nm should be taught about TLS symbols - that they aren't allowed that is
4300120 segment address validation is too simplistic to handle segment
        reservations
4404547 krtld/reloc.h could have better error message, has typos
4270931 R_SPARC_HIX22 relocation is not handled properly
4485320 ld needs to support more the 32768 PLTs
4516434 sotruss can not watch libc_psr.so.1
4213100 sotruss could use more flexible pattern matching
4503457 ld seg fault with comdat
4510264 sections with SHF_TLS can come in different orders...
4518079 link-editor support library unable to modify section header flags
4515913 ld.so.1 can incorrectly decrement external reference counts on dlclose()
4519569 ld -V does not return a interesting value...
4524512 ld.so.1 should allow alternate termination signals
4524767 elfdump dies on bogus sh_name fields...
4524735 ld getopt processing of '-' changed
4521931 subroutine in a shared object as LOCL instead of GLOB
-------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-14
        Solaris/SunOS 5.8_x86           patch 109148-14
        Solaris/SunOS 5.7_sparc         patch 106950-17
        Solaris/SunOS 5.7_x86           patch 106951-17
-------------------------------------------------------------------------------
4532729 tentative definition of TLS variable causes linker to dump core
4526745 fixup ld error message about duplicate dependencies/needed names
4522999 Solaris linker one order of magnitude slower than GNU linker
4518966 dldump undoes existing relocations with no thought of alignment or size.
4587441 Certain libraries have race conditions when setting error codes
4523798 linker option to align bss to large pagesize alignments.
4524008 ld can improperly set st_size of symbols named "_init" or "_fini"
4619282 ld cannot link a program with the option -sb
4620846 Perl Configure probing broken by ld changes
4621122 multiple ld '-zinitarray=' on a commandline fails
-------------------------------------------------------------------------------
        Solaris/SunOS 5.8_sparc         patch 109147-15
        Solaris/SunOS 5.8_x86           patch 109148-15
        Solaris/SunOS 5.7_sparc         patch 106950-18
        Solaris/SunOS 5.7_x86           patch 106951-18
        Solaris/SunOS 5.6_sparc         patch 107733-10
        Solaris/SunOS 5.6_x86           patch 107734-10
-------------------------------------------------------------------------------
All the above changes plus:
        4616944 ar seg faults when order of object file is reversed.
are incorporated in the following patches:
        Solaris/SunOS 5.8_sparc         patch 109147-16
        Solaris/SunOS 5.8_x86           patch 109148-16
-------------------------------------------------------------------------------
All the above changes plus:
        4872634 Large LD_PRELOAD values can cause SEGV of process
are incorporated in the following patches:
        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 inconsistantly 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 symtab 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 (3nd 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 dlmopen(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 dlinfo(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
```

```
4787579 invalid SHT_GROUP entries can cause linker to seg fault
4783869 dlclose: filter closure exhibits hang/failure - introduced with 4504895
4778418 ld.so.1: there be nits out there
4792461 Thread-Local Storage - x86 instruction sequence updates
        PSARC/2002/746 Thread-Local Storage - x86 instruction sequence updates
4461340 sgs: ugly build output while suppressing ia64 (64-bit) build on Intel
4790194 dlopen(..., RTLD_GROUP) has an odd interaction with interposition
4804328 auditing of threaded applications results in deadlock
4806476 building relocatable objects with SHF_EXCLUDE loses relocation
        information
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-06
        Solaris/SunOS 5.9_x86           patch T113986-02
        Solaris/SunOS 5.8_sparc         patch T109147-22
        Solaris/SunOS 5.8_x86           patch T109148-22
--------------------------------------------------------------------------------
4731183 compiler creates .tlsbss section instead of .tbss as documented
4816378 TLS: a tls test case dumps core with C and C++ compilers
4817314 TLS_GD relocations against local symbols do not reference symbol...
4811951 non-default symbol visibility overriden by definition in shared object
4802194 relocation error of mozilla built by K2 compiler
4715815 ld should allow linking with no output file (or /dev/null)
4793721 Need a way to null all code in ISV objects enabling ld performance
        tuning
--------------------------------------------------------------------------------
All the above changes plus:
        4796237 RFE: link-editor became extremely slow with patch 109147-20 and
                static libraries
are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-07
        Solaris/SunOS 5.9_x86           patch T113986-03
        Solaris/SunOS 5.8_sparc         patch T109147-23
        Solaris/SunOS 5.8_x86           patch T109148-23
--------------------------------------------------------------------------------

-------------------------------------
Solaris 9 1203 (5th Q-update - s9u5)
-------------------------------------
Bugid   Risk Synopsis
================================================================================
4830584 mmap for the padding region doesn't get freed after dlclose
4831650 ld.so.1 can walk off the end of it's call_init() array...
4831544 ldd using .so modules compiled with FD7 compiler caused a core dump
4834784 Accessing members in a TLS structure causes a core dump in Oracle
4824026 segv when -z combreloc is used with -xlinkopt
4825296 typo in elfdump
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-08
        Solaris/SunOS 5.9_x86           patch T113986-04
        Solaris/SunOS 5.8_sparc         patch T109147-24
        Solaris/SunOS 5.8_x86           patch T109148-24
--------------------------------------------------------------------------------
4470917 Solaris Process Model Unification (link-editor components only)
        PSARC/2002/117 Solaris Process Model Unification
4744411 Bloomberg wants a faster linker.
4811969 64-bit links can be much slower than 32-bit.
4825065 ld(1) should ignore consecutive empty sections.
4838226 unrelocated shared objects may be erroneously collected for init firing
4830889 TLS: testcase coredumps with -xarch=v9 and -g
4845764 filter removal can leave dangling filtee pointer
4811093 apptrace -F libc date core dumps
4826315 Link editors need to be pre- and post- Unified Process Model aware
4868300 interposing on direct bindings can fail
4872634 Large LD_PRELOAD values can cause SEGV of process
```



```
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-09
        Solaris/SunOS 5.9_x86           patch T113986-05
        Solaris/SunOS 5.8_sparc         patch T109147-25
        Solaris/SunOS 5.8_x86           patch T109148-25
--------------------------------------------------------------------------------

-------------------------------------
Solaris 9 404 (6th Q-update - s9u6)
-------------------------------------
Bugid   Risk Synopsis
================================================================================
4870260 The elfdump command should produce more warning message on invalid move
        entries.
4865418 empty PT_TLS program headers cause problems in TLS enabled applications
4825151 compiler core dumped with a -mt -xF=%all test
4845829 The runtime linker fails to dlopen() long path name.
4900684 shared libraries with more then 32768 plt's fail for sparc ELF64
4906062 Makefiles under usr/src/cmd/sgs needs to be updated
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-10
        Solaris/SunOS 5.9_x86           patch T113986-06
        Solaris/SunOS 5.8_sparc         patch T109147-26
        Solaris/SunOS 5.8_x86           patch T109148-26
        Solaris/SunOS 5.7_sparc         patch T106950-24
        Solaris/SunOS 5.7_x86           patch T106951-24
--------------------------------------------------------------------------------
4900320 rtld library mapping could be faster
4911775 implement GOTDATA proposal in ld
        PSARC/2003/477 SPARC GOTDATA instruction sequences
4904565 Functionality to ignore relocations against external symbols
4764817 add section types SHT_DEBUG and SHT_DEBUGSTR
        PSARC/2003/510 New ELF DEBUG and ANNOTATE sections
4850703 enable per-symbol direct bindings
4716275 Help required in the link analysis of runtime interfaces
        PSARC/2003/519 Link-editors: Direct Binding Updates
4904573 elfdump may hang when processing archive files
4918310 direct binding from an executable can't be interposed on
4918938 ld.so.1 has become SPARC32PLUS - breaks 4.x binary compatibility
4911796 S1S8 C++: ld dump core when compiled and linked with xlinkopt=1.
4889914 ld crashes with SEGV using -M mapfile under certain conditions
4911936 exception are not catch from shared library with -zignore
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-11
        Solaris/SunOS 5.9_x86           patch T113986-07
        Solaris/SunOS 5.8_sparc         patch T109147-27
        Solaris/SunOS 5.8_x86           patch T109148-27
        Solaris/SunOS 5.7_sparc         patch T106950-25
        Solaris/SunOS 5.7_x86           patch T106951-25
--------------------------------------------------------------------------------
4946992 ld crashes due to huge number of sections (>65,000)
4951840 mcs -c goes into a loop on executable program
4939869 Need additional relocation types for abs34 code model
        PSARC/2003/684 abs34 ELF relocations
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-12
        Solaris/SunOS 5.9_x86           patch T113986-08
        Solaris/SunOS 5.8_sparc         patch T109147-28
        Solaris/SunOS 5.8_x86           patch T109148-28
--------------------------------------------------------------------------------

-------------------------------------
```

```
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 $ISALIST/$HWCAP expansion should be more flexible.
875 4918303 0@0.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 relocs 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 Broadvison 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 .plts (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 coredumps 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 libdl 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 hwcap filtee
 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         rtld/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) -Bnodirect 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 mulitiply 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_ARGSINFO
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 --------------------------------------------------------------------------------
```

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.9_sparc	patch T112963-24
Solaris/SunOS 5.9_x86	patch T113986-20
Solaris/SunOS 5.8_sparc	patch T109147-39
Solaris/SunOS 5.8_x86	patch T109148-39

6318306 a dlsym() from a filter should be redirected to an associated filtee
6318401 mis-aligned TLS variable
6324019 ld.so.1: malloc alignment is insufficient for new compilers
6324589 psh coredumps on x86 machines on snv_23
6236594 AMD64: Linker needs to handle the new .lbss section (D)
PSARC 2005/514 AMD64 - large section support
6314743 Linker: incorrect resolution for R_AMD64_GOTPC32
6311865 Linker: x86 medium model; invalid ELF program header

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.10_sparc	patch T117461-07
Solaris/SunOS 5.10_x86	patch T118345-12

6309061 link_audit should use __asm__ with gcc
6310736 gcc and sgs/libld don’t get along on SPARC
6329796 Memory leak with iconv_open/iconv_close with patch 109147-33
6332983 s9 linker patches 112963-24/113986-20 causing cluster machines not
to boot

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.10_sparc	patch T117461-08
Solaris/SunOS 5.10_x86	patch T121208-02
Solaris/SunOS 5.9_sparc	patch T112963-25
Solaris/SunOS 5.9_x86	patch T113986-21
Solaris/SunOS 5.8_sparc	patch T109147-40
Solaris/SunOS 5.8_x86	patch T109148-40

6445311 The sparc S8/S9/S10 linker patches which include the fix for the
CR6222525 are hit by the CR6439613.

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.9_sparc	patch T112963-26
Solaris/SunOS 5.8_sparc	patch T109147-41

Solaris 10 807 (4th Q-update - s10u4)

Bugid Risk Synopsis

6487273 ld.so.1 may open arbitrary locale files when relative path is built
from locale environment vars
6487284 ld.so.1: buffer overflow in doprf() function

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.10_sparc	patch T124922-01
Solaris/SunOS 5.10_x86	patch T124923-01
Solaris/SunOS 5.9_sparc	patch T112963-27
Solaris/SunOS 5.9_x86	patch T113986-22
Solaris/SunOS 5.8_sparc	patch T109147-42
Solaris/SunOS 5.8_x86	patch T109148-41

6477132 ld.so.1: memory leak when running set*id application

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.10_sparc	patch T124922-02
Solaris/SunOS 5.10_x86	patch T124923-02
Solaris/SunOS 5.9_sparc	patch T112963-30
Solaris/SunOS 5.9_x86	patch T113986-24

6340814 ld.so.1 core dump with HWCAP relocatable object + updated statistics
6307274 crle bug with LD_LIBRARY_PATH
6317969 elfheader limited to 65535 segments (link-editor components only)
6350027 ld.so.1 aborts with assertion failed on amd64
6362044 ld(1) inconsistencies with LD_DEBUG=-Dunused and -zignore
6362047 ld.so.1 dumps core when combining HWCAP and LD_PROFILE
6304206 runtime linker may respect LANG and LC_MESSAGE more than LC_ALL
6363495 Catchup required with Intel relocations
6326497 ld.so not properly processing LD_LIBRARY_PATH ending in :
6307146 mcs dumps core when appending null string to comment section
6371877 LD_PROFILE_64 with gprof does not produce correct results on amd64
6372082 ld -r erroneously creates .got section on i386
6201866 amd64: linker symbol elimination is broken
6372620 printstack() segfaults when called from static function (D)
6380470 32-bit ld(1) incorrectly builds 64-bit relocatable objects
6391407 Insufficient alignment of 32-bit object in archive makes ld segfault
(libelf component only) (D)
6316708 LD_DEBUG should provide a means of identifying/isolating individual
link-map lists (P)
6280209 elfdump cores on memory model 0x3
6197234 elfdump and dump don’t handle 64-bit symbols correctly
6398893 Extended section processing needs some work
6397256 ldd dumps core in elf_fix_name
6327926 ld does not set etext symbol correctly for AMD64 medium model (D)
6390410 64-bit LD_PROFILE can fail: relocation error when binding profile plt
6382945 AMD64-GCC: dbx: internal error: dwarf reference attribute out of bounds
6262333 init section of .so dlopened from audit interface not being called
6409613 elf_outsync() should fsync()
6426048 C++ exceptions broken in Nevada for amd64
6429418 ld.so.1: need work-around for Nvidia drivers use of static TLS
6429504 crle(1) shows wrong defaults for non-existent 64-bit config file
6431835 data corruption on x64 in 64-bit mode while LD_PROFILE is in effect
6423051 static TLS support within the link-editors needs a major face lift (D)
6388946 attempting to dlopen a .o file mislabeled as .so fails
6446740 allow mapfile symbol definitions to create backing storage (D)
4986360 linker crash on exec of .so (as opposed to a.out) -- error preferred
instead
6229145 ld: initarray/finiarray processing occurs after got size is determined
6324924 the linker should warn if there’s a .init section but not _init
6424132 elfdump inserts extra whitespace in bitmap value display
6449485 ld(1) creates misaligned TLS in binary compiled with -xpg
6424550 Write to unallocated (wua) errors when libraries are built with
-z lazyload
6464235 executing the 64-bit ld(1) should be easy (D)
6465623 need a way of building unix without an interpreter
6467925 ld: section deletion (-z ignore) requires improvement
6357230 specfiles should be nuked (link-editor components only)

All the above changes are incorporated in the following patches:

Solaris/SunOS 5.10_sparc	patch T124922-03
Solaris/SunOS 5.10_x86	patch T124923-03

These patches also include the framework changes for the following bug fixes.
However, the associated feature has not been enabled in Solaris 10 or earlier
releases:

6174390 crle configuration files are inconsistent across platforms (D, P)
6432984 ld(1) output file removal - change default behavior (D)
PSARC/2006/353 ld(1) output file removal - change default behavior

---

Solaris 10 508 (5th Q-update - s10u5)

Bugid Risk Synopsis

```
6561987 data vac_conflict faults on lipthread libthread libs in s10.
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T127111-01
        Solaris/SunOS 5.10_x86          patch T127112-01
--------------------------------------------------------------------------------
6501793 GOTOP relocation transition (optimization) fails with offsets > 2^32
6532924 AMD64: Solaris 5.11 55b: SEGV after whocatches
6551627 OGL: SIGSEGV when trying to use OpenGL pipeline with splash screen,
        Solaris/Nvidia only
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T127111-04
        Solaris/SunOS 5.10_x86          patch T127112-04
--------------------------------------------------------------------------------
6479848 Enhancements to the linker support interface needed. (D)
        PSARC/2006/595 link-editor support library interface - ld_open()
6521608 assertion failure in runtime linker related to auditing
6494228 pclose() error when an audit library calls popen() and the main target
        is being run under ldd (D)
6568745 segfault when using LD_DEBUG with bit_audit library when instrumenting
        mozilla (D)
        PSARC/2007/413 Add -zglobalaudit option to ld
6602294 ps_pbrandname breaks apps linked directly against librtld_db
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T127111-07
        Solaris/SunOS 5.10_x86          patch T127112-07
--------------------------------------------------------------------------------

------------------------------------
Solaris 10 908 (6th Q-update - s10u6)
------------------------------------
Bugid   Risk Synopsis
================================================================================
6672544 elf_rtbndr must support non-ABI aligned stacks on amd64
6668050 First trip through PLT does not preserve args in xmm registers
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patch:
        Solaris/SunOS 5.10_x86          patch T137138-01
--------------------------------------------------------------------------------

------------------------------------
Solaris 10 409 (7th Q-update - s10u7)
------------------------------------
Bugid   Risk Synopsis
================================================================================
6629404 ld with -z ignore doesn't scale
6606203 link editor ought to allow creation of >2gb sized objects (P)
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T139574-01
        Solaris/SunOS 5.10_x86          patch T139575-01
--------------------------------------------------------------------------------
6746674 setuid applications do not find libraries any more because trusted
        directories behavior changed (D)
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T139574-02
        Solaris/SunOS 5.10_x86          patch T139575-02
--------------------------------------------------------------------------------
6703683 Can't build VirtualBox on Build 88 or 89
6737579 process_req_lib() in libld consumes file descriptors
6685125 ld/elfdump do not handle ZERO terminator .eh_frame amd64 unwind entry
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
```



```
        Solaris/SunOS 5.10_sparc        patch T139574-03
        Solaris/SunOS 5.10_x86          patch T139575-03
--------------------------------------------------------------------------------

------------------------------------
Solaris 10 1009 (8th Q-update - s10u8)
------------------------------------
Bugid   Risk Synopsis
================================================================================
6782597 32-bit ld.so.1 needs to accept objects with large inode number
6805502 The addition of "inline" keywords to sgs code broke the lint
        verification in S10
6807864 ld.so.1 is susceptible to a fatal dlsym()/setlocale() race
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T141692-01
        Solaris/SunOS 5.10_x86          patch T141693-01
NOTE: The fix for 6805502 is only applicable to s10.
--------------------------------------------------------------------------------
6826410 ld needs to sort sections using 32-bit sort keys
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T141771-01
        Solaris/SunOS 5.10_x86          patch T141772-01
NOTE: The fix for 6826410 is also available for s9 in the following patches:
        Solaris/SunOS 5.9_sparc         patch T112963-33
        Solaris/SunOS 5.9_x86           patch T113986-27
--------------------------------------------------------------------------------
6568447 bcp is broken by 6551627
6599700 librtld_db needs better plugin support
6713830 mdb dumped core reading a gcore
6756048 rd_loadobj_iter() should always invoke brand plugin callback
6786744 32-bit dbx failed with unknown rtld_db.so error on snv_104
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T141444-06
        Solaris/SunOS 5.10_x86          patch T141445-06
--------------------------------------------------------------------------------

------------------------------------
Solaris 10 1005 (9th Q-update - s10u9)
------------------------------------
Bugid   Risk Synopsis
================================================================================
6850124 dlopen reports "No such file or directory" in spite of ENOMEM
        when mmap fails in anon_map()
6826513 ldd gets confused by a crle(1) LD_PRELOAD setting
6684577 ld should propagate SHF_LINK_ORDER flag to ET_REL objects
6524709 executables using /usr/lib/libc.so.1 as the ELF interpreter dump core
        (link-editor components only)
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch T143895-01
        Solaris/SunOS 5.10_x86          patch T143896-01
--------------------------------------------------------------------------------

------------------------------------
Solaris 10 XXXX (10th Q-update - s10u10)
------------------------------------
Bugid   Risk Synopsis
================================================================================
6478684 isainfo/cpuid reports pause instruction not supported on amd64
        PSARC/2010/089 Removal of AV_386_PAUSE and AV_386_MON
--------------------------------------------------------------------------------
All the above changes are incorporated in the following patches:
        Solaris/SunOS 5.10_sparc        patch TXXXXXX-XX
```

```
        Solaris/SunOS 5.10_x86          patch TXXXXXX-XX
--------------------------------------------------------------------------------

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



```
6565476 rtld symbol version check prevents GNU ld binary from running
6567670 ld(1) symbol size/section size verification uncovers Haskell
        compiler inconsistency
6530249 elfdump should handle ELF files with no section header table (D)
        PSARC/2007/395 Add -P option to elfdump
6573641 ld.so.1 does not maintain parent relationship to a dlopen() caller.
6577462 Additional improvements needed to handling of gcc's symbol versioning
6583742 ELF string conversion library needs to lose static writable buffers
6589819 ld generated reference to __tls_get_addr() fails when resolving to a
        shared object reference
6595139 various applications should export yy* global variables for libl
        PSARC/2007/474 new ldd(1) -w option
6597841 gelf_getdyn() reads one too many dynamic entries
6603313 dlclose() can fail to unload objects after fix for 6573641
6234471 need a way to edit ELF objects (D)
        PSARC/2007/509 elfedit
5035454 mixing -Kpic and -KPIC may cause SIGSEGV with -xarch=v9
6473571 strip and mcs get confused and corrupt files when passed
        non-ELF arguments
6253589 mcs has problems handling multiple SHT_NOTE sections
6610591 do_reloc() should not require unused arguments
6602451 new symbol visibilities required: EXPORTED, SINGLETON and ELIMINATE (D)
        PSARC/2007/559 new symbol visibilities - EXPORTED, SINGLETON, and
        ELIMINATE
6570616 elfdump should display incorrectly aligned note section
6614968 elfedit needs string table module (D)
6620533 HWCAP filtering can leave uninitialized data behind - results in
        "rejected: Invalid argument"
6617855 nodirect tag can be ignored when other syminfo tags are available
        (link-editor components only)
6621066 Reduce need for new elfdump options with every section type (D)
        PSARC/2007/620 elfdump -T, and simplified matching
6627765 soffice failure after integration of 6603313 - dangling GROUP pointer.
6319025 SUNWbtool packaging issues in Nevada and S10u1.
6626135 elfedit capabilities str->value mapping should come from
        usr/src/common/elfcap
6642769 ld(1) -z combreloc should become default behavior (D)
        PSARC/2008/006 make ld(1) -z combreloc become default behavior
6634436 XFFLAG should be updated.  (link-editor components only)
6492726 Merge SHF_MERGE|SHF_STRINGS input sections (D)
4947191 OSNet should use direct bindings  (link-editor components only)
6654381 lazy loading fall-back needs optimizing
6658385 ld core dumps when building Xorg on nv_82
6516808 ld.so.1's token expansion provides no escape for platforms that don't
        report HWCAP
6668534 Direct bindings can compromise function address comparisons from
        executables
6667661 Direct bindings can compromise executables with insufficient copy
        relocation information
6357282 ldd should recognize PARENT and EXTERN symbols (D)
        PSARC/2008/148 new ldd(1) -p option
6672394 ldd(1) unused dependency processing is tricked by relocations errors
--------------------------------------------------------------------------------

----------------------------------------
Solaris Nevada (OpenSolaris 2008.11, snv_101)
----------------------------------------
Bugid   Risk Synopsis
================================================================================
6671255 link-editor should support cross linking (D)
        PSARC/2008/179 cross link-editor
6674666 elfedit dyn:posflag1 needs option to locate element via NEEDED item
6675591 elfwrap - wrap data in an ELF file (D,P)
        PSARC/2008/198 elfwrap - wrap data in an ELF file
6678244 elfdump dynamic section sanity checking needs refinement
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 develpment
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 coredumps 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 allextract 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 allextract 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 sgsmsg 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    dldump() 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    rtld _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 10471   ld(1) amd64 LD->LE TLS transition causes memory corruption
1666 #endif /* ! codereview */
```

****
2644 Thu Feb 28 22:40:43 2019
new/usr/src/pkg/manifests/system-test-elftest.mf
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright 2018, Richard Lowe.
#

set name=pkg.fmri value=pkg:/system/test/elftest@$(PKGVERS)
set name=pkg.description value="ELF Unit Tests"
set name=pkg.summary value="ELF Test Suite"
set name=info.classification \
    value=org.opensolaris.category.2008:Development/System
set name=variant.arch value=$(ARCH)
dir path=opt/elf-tests
dir path=opt/elf-tests/bin
dir path=opt/elf-tests/runfiles
dir path=opt/elf-tests/tests
dir path=opt/elf-tests/tests/assert-deflib
dir path=opt/elf-tests/tests/tls
dir path=opt/elf-tests/tests/tls/amd64
dir path=opt/elf-tests/tests/tls/amd64/ie
dir path=opt/elf-tests/tests/tls/amd64/ld
dir path=opt/elf-tests/tests/tls/i386
dir path=opt/elf-tests/tests/tls/i386/ld
file path=opt/elf-tests/README mode=0444
file path=opt/elf-tests/bin/elftest mode=0555
file path=opt/elf-tests/runfiles/default.run mode=0444
file path=opt/elf-tests/tests/assert-deflib/link.c mode=0444
file path=opt/elf-tests/tests/assert-deflib/test-deflib mode=0555
file path=opt/elf-tests/tests/tls/amd64/ie/Makefile.test mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/amd64-ie-test mode=0555
file path=opt/elf-tests/tests/tls/amd64/ie/style1-func-with-r12.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style1-func-with-r13.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style1-func.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style1-main.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style2-with-badness.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style2-with-r12.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style2-with-r13.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ie/style2.s mode=0444
file path=opt/elf-tests/tests/tls/amd64/ld/Makefile.test mode=0444
file path=opt/elf-tests/tests/tls/amd64/ld/amd64-ld-test mode=0555
file path=opt/elf-tests/tests/tls/amd64/ld/ld-with-addend.s mode=0444
file path=opt/elf-tests/tests/tls/i386/ld/Makefile.test mode=0444
file path=opt/elf-tests/tests/tls/i386/ld/half-ldm.s mode=0444
file path=opt/elf-tests/tests/tls/i386/ld/i386-ld-test mode=0555
license lic_CDDL license=lic_CDDL
depend fmri=developer/linker type=require
depend fmri=developer/object-file type=require
depend fmri=system/test/testrunner type=require
#endif /* ! codereview */
```

****
687 Thu Feb 28 22:40:44 2019
new/usr/src/test/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012 by Delphix. All rights reserved.
# Copyright 2014 Garrett D'Amore <garrett@damore.org>
#

.PARALLEL: $(SUBDIRS)

SUBDIRS = \
        crypto-tests \
        elf-tests \
        libc-tests \
        os-tests \
        smbclient-tests \
        test-runner \
        util-tests \
        zfs-tests
SUBDIRS = libc-tests crypto-tests os-tests test-runner util-tests zfs-tests \
        smbclient-tests

include Makefile.com
```

```
**********************************************************
     559 Thu Feb 28 22:40:44 2019
new/usr/src/test/elf-tests/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
   1 #
   2 # This file and its contents are supplied under the terms of the
   3 # Common Development and Distribution License ("CDDL"), version 1.0.
   4 # You may only use this file in accordance with the terms of version
   5 # 1.0 of the CDDL.
   6 #
   7 # A full copy of the text of the CDDL should have accompanied this
   8 # source.  A copy of the CDDL is also available via the Internet at
   9 # http://www.illumos.org/license/CDDL.
  10 #

  12 #
  13 # Copyright 2015 Nexenta Systems, Inc.  All rights reserved.
  14 #

  16 .PARALLEL: $(SUBDIRS)

  18 SUBDIRS = cmd doc runfiles tests

  20 include $(SRC)/test/Makefile.com
  21 #endif /* ! codereview */
```

```
**********************************************************
     852 Thu Feb 28 22:40:44 2019
new/usr/src/test/elf-tests/cmd/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012 by Delphix. All rights reserved.
# Copyright 2015 Nexenta Systems, Inc.  All rights reserved.
#

include $(SRC)/Makefile.master
include $(SRC)/test/Makefile.com

ROOTOPTPKG = $(ROOT)/opt/elf-tests
ROOTBIN = $(ROOTOPTPKG)/bin

PROGS = elftest

CMDS = $(PROGS:%=$(ROOTBIN)/%)
$(CMDS) := FILEMODE = 0555

all lint clean clobber:

install: $(CMDS)

$(CMDS): $(ROOTBIN)

$(ROOTBIN):
        $(INS.dir)

$(ROOTBIN)/%: %.ksh
        $(INS.rename)
#endif /* ! codereview */
```

```
**********************************************************
     983 Thu Feb 28 22:40:45 2019
new/usr/src/test/elf-tests/cmd/elftest.ksh
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#!/usr/bin/ksh

#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright 2015 Nexenta Systems, Inc.  All rights reserved.
#

ELF_TESTS="/opt/elf-tests"
runner="/opt/test-runner/bin/run"

function fail
{
        echo $1
        exit ${2:-1}
}

function find_runfile
{
        typeset distro=default

        [[ -n $distro ]] && echo $ELF_TESTS/runfiles/$distro.run
}

while getopts c: c; do
        case $c in
        'c')
                runfile=$OPTARG
                [[ -f $runfile ]] || fail "Cannot read file: $runfile"
                ;;
        esac
done
shift $((OPTIND - 1))

[[ -z $runfile ]] && runfile=$(find_runfile)
[[ -z $runfile ]] && fail "Couldn't determine distro"

$runner -c $runfile

exit $?
#endif /* ! codereview */
```

```
**********************************************************
     806 Thu Feb 28 22:40:45 2019
new/usr/src/test/elf-tests/doc/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
   1 #
   2 # This file and its contents are supplied under the terms of the
   3 # Common Development and Distribution License ("CDDL"), version 1.0.
   4 # You may only use this file in accordance with the terms of version
   5 # 1.0 of the CDDL.
   6 #
   7 # A full copy of the text of the CDDL should have accompanied this
   8 # source.  A copy of the CDDL is also available via the Internet at
   9 # http://www.illumos.org/license/CDDL.
  10 #

  12 #
  13 # Copyright (c) 2012 by Delphix. All rights reserved.
  14 # Copyright 2015 Nexenta Systems, Inc.  All rights reserved.
  15 #

  17 include $(SRC)/Makefile.master

  19 README = README

  21 ROOTOPTPKG = $(ROOT)/opt/elf-tests

  23 FILES = $(README:%=$(ROOTOPTPKG)/%)
  24 $(FILES) := FILEMODE = 0444

  26 all: $(README)

  28 install: $(ROOTOPTPKG) $(FILES)

  30 clean lint clobber:

  32 $(ROOTOPTPKG):
  33         $(INS.dir)

  35 $(ROOTOPTPKG)/%: %
  36         $(INS.file)
  37 #endif /* ! codereview */
```

```
**********************************************************
    2003 Thu Feb 28 22:40:45 2019
new/usr/src/test/elf-tests/doc/README
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012 by Delphix. All rights reserved.
# Copyright 2015 Nexenta Systems, Inc.  All rights reserved.
#

ELF Software Generation Utilities Unit Test Suite README

1. Building and installing the ELF/SGS Unit Test Suite
2. Running the ELF/SGS Unit Test Suite
3. Test results

--------------------------------------------------------------------------------

1. Building and installing the ELF/SGS Unit Test Suite

The ELF/SGS Unit Test Suite runs under the testrunner framework (which can be
installed as pkg:/system/test/testrunner). To build both the ELF/SGS Unit Test S
and the testrunner without running a full nightly:

        build_machine$ bldenv [-d] <your_env_file>
        build_machine$ cd $SRC/test
        build_machine$ dmake install
        build_machine$ cd $SRC/pkg
        build_machine$ dmake install

Then set the publisher on the test machine to point to your repository and
install the ELF/SGS Unit Test Suite.

        test_machine# pkg install pkg:/system/test/elftest

Note, the framework will be installed automatically, as the ELF/SGS Unit Test Su
depends on it.

2. Running the ELF/SGS Unit Test Suite

The pre-requisites for running the ELF/SGS Unit Test Suite are:
    None

Once the pre-requisites are satisfied, simply run the elftest script:

        test_machine$ /opt/elf-tests/bin/elftest

3. Test results

While the ELF/SGS Unit Test Suite is running, one informational line is printed
the end of each test, and a results summary is printed at the end of the run.
The results summary includes the location of the complete logs, which is of the
form /var/tmp/test_results/<ISO 8601 date>.
#endif /* ! codereview */
```

```
**********************************************************
     908 Thu Feb 28 22:40:45 2019
new/usr/src/test/elf-tests/runfiles/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012 by Delphix. All rights reserved.
# Copyright 2014, OmniTI Computer Consulting, Inc. All rights reserved.
# Copyright 2014 Garrett D'Amore <garrett@damore.org>
#

include $(SRC)/Makefile.master

SRCS = default.run

ROOTOPTPKG = $(ROOT)/opt/elf-tests
RUNFILES = $(ROOTOPTPKG)/runfiles

CMDS = $(SRCS:%=$(RUNFILES)/%)
$(CMDS) := FILEMODE = 0444

all: $(SRCS)

install: $(CMDS)

clean lint clobber:

$(CMDS): $(RUNFILES) $(SRCS)

$(RUNFILES):
        $(INS.dir)

$(RUNFILES)/%: %
        $(INS.file)
#endif /* ! codereview */
```

```
**********************************************************
     826 Thu Feb 28 22:40:45 2019
new/usr/src/test/elf-tests/runfiles/default.run
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2018, Richard Lowe.

[DEFAULT]
pre =
verbose = False
quiet = False
timeout = 60
post =
outputdir = /var/tmp/test_results

[/opt/elf-tests/tests/assert-deflib]
tests = ['test-deflib']


[/opt/elf-tests/tests/tls/amd64/ie]
arch = i86pc
tests = ['amd64-ie-test']

[/opt/elf-tests/tests/tls/i386/ld]
arch = i86pc
tests = ['i386-ld-test']

[/opt/elf-tests/tests/tls/amd64/ld]
arch = i86pc
tests = ['amd64-ld-test']
#endif /* ! codereview */
```

****
567 Thu Feb 28 22:40:46 2019
new/usr/src/test/elf-tests/tests/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012, 2016 by Delphix. All rights reserved.
# Copyright 2018 Joyent, Inc.
#

SUBDIRS =               \
        assert-deflib   \
        tls

include $(SRC)/test/Makefile.com
#endif /* ! codereview */
```

```
**********************************************************
     939 Thu Feb 28 22:40:46 2019
new/usr/src/test/elf-tests/tests/assert-deflib/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2018, Richard Lowe.

include $(SRC)/cmd/Makefile.cmd
include $(SRC)/test/Makefile.com

PROG =  test-deflib

DATAFILES =     link.c

ROOTOPTPKG = $(ROOT)/opt/elf-tests
TESTDIR = $(ROOTOPTPKG)/tests/assert-deflib

CMDS = $(PROG:%=$(TESTDIR)/%)
$(CMDS) := FILEMODE = 0555

DATA = $(DATAFILES:%=$(TESTDIR)/%)
$(DATA) := FILEMODE = 0444

all: $(PROG)

install: all $(CMDS) $(DATA)

lint:

clobber: clean
        -$(RM) $(PROG)

clean:
        -$(RM) $(CLEANFILES)

$(CMDS): $(TESTDIR) $(PROG)

$(TESTDIR):
        $(INS.dir)

$(TESTDIR)/%: %
        $(INS.file)
#endif /* ! codereview */
```

```
**********************************************************
    3768 Thu Feb 28 22:40:46 2019
new/usr/src/test/elf-tests/tests/assert-deflib/test-deflib.sh
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#!/bin/bash
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012, Joyent, Inc.
#

#
# This test validates that the -zassert-deflib option of ld(1) works correctly.
# It requires that some cc is in your path and that you have passed in the path
# to the proto area with the new version of libld.so.4. One thing that we have
# to do is be careful with using LD_LIBRARY_PATH. Setting LD_LIBRARY_PATH does
# not change the default search path so we want to make sure that we use a
# different ISA (e.g. 32-bit vs 64-bit) from the binary we're generating.
#
unalias -a

TESTDIR=$(dirname $0)

#endif /* ! codereview */
sh_path=
sh_lib="lib"
sh_lib64="$sh_lib/64"
sh_soname="libld.so.4"
sh_cc="gcc"
sh_cc="cc"
sh_cflags="-m32"
sh_file="${TESTDIR}/link.c"
sh_file="link.c"
sh_arg0=$(basename $0)

function fatal
{
        local msg="$*"
        [[ -z "$msg" ]] && msg="failed"
        echo "$sh_arg0: $msg" >&2
        exit 1
}
```

_____*unchanged_portion_omitted_*

```
sh_path=${1:-/}
sh_path=$1
[[ -z "$1" ]] && fatal "<proto root>"
validate

run "-Wl,-zassert-deflib" 0 \
    "Testing basic compilation succeeds with warnings..." \
    "failed to compile with warnings"

run "-Wl,-zassert-deflib -Wl,-zfatal-warnings" 1 \
    "Testing basic compilation fails if warning are fatal..." \
```



```
    "linking succeeeded, expected failure"

run "-Wl,-zassert-deflib=libc.so -Wl,-zfatal-warnings" 0 \
    "Testing basic exception with fatal warnings..." \
    "linking failed despite exception"

run "-Wl,-zassert-deflib=libc.so -Wl,-zfatal-warnings" 0 \
    "Testing basic exception with fatal warnings..." \
    "linking failed despite exception"


run "-Wl,-zassert-deflib=lib.so -Wl,-zfatal-warnings" 1 \
    "Testing invalid library name..." \
    "ld should not allow invalid library name"

run "-Wl,-zassert-deflib=libf -Wl,-zfatal-warnings" 1 \
    "Testing invalid library name..." \
    "ld should not allow invalid library name"

run "-Wl,-zassert-deflib=libf.s -Wl,-zfatal-warnings" 1 \
    "Testing invalid library name..." \
    "ld should not allow invalid library name"

run "-Wl,-zassert-deflib=libc.so -Wl,-zfatal-warnings -lelf" 1 \
    "Errors even if one library is under exception path..." \
    "one exception shouldn't stop another"

args="-Wl,-zassert-deflib=libc.so -Wl,-zassert-deflib=libelf.so"
args="$args -Wl,-zfatal-warnings -lelf"

run "$args" 0 \
    "Multiple exceptions work..." \
    "multiple exceptions don't work"

args="-Wl,-zassert-deflib=libc.so -Wl,-zassert-deflib=libelfe.so"
args="$args -Wl,-zfatal-warnings -lelf"

run "$args" 1 \
    "Exceptions only catch the specific library" \
    "exceptions caught the wrong library"

args="-Wl,-zassert-deflib=libc.so -Wl,-zassert-deflib=libel.so"
args="$args -Wl,-zfatal-warnings -lelf"

run "$args" 1 \
    "Exceptions only catch the specific library" \
    "exceptions caught the wrong library"

echo "Tests passed."
exit 0
```

****
553 Thu Feb 28 22:40:47 2019
new/usr/src/test/elf-tests/tests/tls/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012, 2016 by Delphix. All rights reserved.
# Copyright 2018 Joyent, Inc.
#

SUBDIRS = amd64 i386

include $(SRC)/test/Makefile.com
#endif /* ! codereview */
```

****
548 Thu Feb 28 22:40:47 2019
new/usr/src/test/elf-tests/tests/tls/amd64/Makefile
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012, 2016 by Delphix. All rights reserved.
# Copyright 2018 Joyent, Inc.
#

SUBDIRS = ie ld

include $(SRC)/test/Makefile.com
#endif /* ! codereview */
```

```
**********************************************************
    1121 Thu Feb 28 22:40:47 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2018, Richard Lowe.

include $(SRC)/cmd/Makefile.cmd
include $(SRC)/test/Makefile.com

PROG =  amd64-ie-test

DATAFILES =                     \
        Makefile.test           \
        style1-func-with-r12.s  \
        style1-func-with-r13.s  \
        style1-func.s           \
        style1-main.s           \
        style2-with-badness.s   \
        style2-with-r12.s       \
        style2-with-r13.s       \
        style2.s

ROOTOPTPKG = $(ROOT)/opt/elf-tests
TESTDIR = $(ROOTOPTPKG)/tests/tls/amd64/ie

CMDS = $(PROG:%=$(TESTDIR)/%)
$(CMDS) := FILEMODE = 0555


DATA = $(DATAFILES:%=$(TESTDIR)/%)
$(DATA) := FILEMODE = 0444

all: $(PROG)

install: all $(CMDS) $(DATA)

lint:

clobber: clean
        -$(RM) $(PROG)

clean:
        -$(RM) $(CLEANFILES)

$(CMDS): $(TESTDIR) $(PROG)

$(TESTDIR):
        $(INS.dir)

$(TESTDIR)/%: %
        $(INS.file)
#endif /* ! codereview */
```

```
**********************************************************
    2251 Thu Feb 28 22:40:47 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/Makefile.test
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

CC =            gcc
include $(SRC)/Makefile.master

# We have to use GCC, and only GCC.  The best way is to ask cw(1) which GCC to u
CC_CMD =        $(ONBLD_TOOLS)/bin/$(MACH)/cw -_gcc -_compiler
CC =            $(CC_CMD:sh)
CFLAGS =        -O1 -m64

LINK.c =  $(CC) $(CFLAGS) -o $@ $^
LINK.c = env LD_ALTEXEC=$(PROTO)/usr/bin/amd64/ld $(CC) $(CFLAGS) -o $@ $^
COMPILE.c = $(CC) $(CFLAGS) -c -o $@ $^
COMPILE.s = $(CC) $(CFLAGS) -c -o $@ $^

.KEEP_STATE:

install default: all

%.o: $(TESTDIR)/%.s
.c.o:
        $(COMPILE.c)

.s.o:
        $(COMPILE.s)

# A basic use of TLS that uses the movq m/r --> movq i/r variant
PROGS +=        style2
STYLE2OBJS =    style2.o
style2: $(STYLE2OBJS)
        $(LINK.c)

# A copy of style2 that uses %r13 in the TLS sequence, and thus excercises the
# REX transitions of the movq mem,reg -> movq imm,reg variant.
PROGS +=        style2-with-r13
STYLE2R13OBJS = style2-with-r13.o
style2-with-r13: $(STYLE2R13OBJS)
        $(LINK.c)

# A copy of style2 that uses %r12 in the TLS sequence, so we can verify that
# it is _not_ special to this variant
PROGS +=        style2-with-r12
STYLE2R12OBJS = style2-with-r12.o
style2-with-r12: $(STYLE2R12OBJS)
        $(LINK.c)

# A copy of style2 that has a R_AMD64_GOTTPOFF relocation with a bad insn sequen
STYLE2BADNESSOBJS =     style2-with-badness.o
style2-with-badness: $(STYLE2BADNESSOBJS)
```



```
        -$(LINK.c)

# A basic use of TLS that uses the addq mem/reg --> leaq mem,reg variant
PROGS +=        style1
STYLE1OBJS =    style1-main.o style1-func.o
style1: $(STYLE1OBJS)
        $(LINK.c)

# A copy of style1-func that uses %r13 in the TLS sequence and thus excercises
# the REX transitions. of the addq mem,reg --> leaq mem,reg variant
PROGS +=        style1-with-r13
STYLE1R13OBJS = style1-main.o style1-func-with-r13.o
style1-with-r13: $(STYLE1R13OBJS)
        $(LINK.c)

# A copy of style1-func that uses %r12 to test the addq mem,reg --> addq imm,reg
PROGS +=        style1-with-r12
STYLE1R12OBJS = style1-main.o style1-func-with-r12.o
style1-with-r12: $(STYLE1R12OBJS)
        $(LINK.c)

all:    $(PROGS)

clobber clean:
        rm -f $(PROGS) $(STYLE1OBJS) $(STYLE1R13OBJS) $(STYLE1R12OBJS) \
            $(STYLE2OBJS) $(STYLE2R13OBJS) $(STYLE2R12OBJS) $(STYLE2BADNESSOBJS)

fail: style2-with-badness FRC

FRC:
```

```
**********************************************************
     210 Thu Feb 28 22:40:48 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/README
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
   1 This tests the amd64 link-editor's handling of Initial Executable TLS sequences.

   3 The original C source files are in orig/ but unused, since we need to avoid
   4 any changes to the compiler influencing our tests.

   6 #endif /* ! codereview */
```

```
**********************************************************
    2170 Thu Feb 28 22:40:48 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/amd64-ie-test.sh
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#!/bin/ksh
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

function grep_test {
    name=$1
    pattern=$2

    if /usr/bin/fgrep -q "${pattern}"; then
        print -u2 "pass: $name"
    else
        print -u2 "FAIL: $name"
        exit 1
#endif /* ! codereview */
    fi
}

function dis_test {
    name=${1}
    func=${2}
    file=${3}
    pattern=${4}

    dis -F${func} ${file} | grep_test "${name}" "${pattern}"
}

TESTDIR=$(dirname $0)
make -f ${TESTDIR}/Makefile.test TESTDIR=${TESTDIR}
make PROTO="${1}"

dis_test "addq-->leaq 1" func style1 \
    'func+0x10: 48 8d 92 f8 ff ff  leaq   -0x8(%rdx),%rdx'
dis_test "addq-->leaq 2" func style1 \
    'func+0x17: 48 8d b6 f0 ff ff  leaq   -0x10(%rsi),%rsi'

dis_test "addq-->leaq w/REX 1" func style1-with-r13 \
    'func+0x10: 48 8d 92 f8 ff ff  leaq   -0x8(%rdx),%rdx'
dis_test "addq-->leaq w/REX 2" func style1-with-r13 \
    'func+0x17: 4d 8d ad f0 ff ff  leaq   -0x10(%r13),%r13'

dis_test "addq-->addq for SIB 1" func style1-with-r12 \
    'func+0x10: 48 8d 92 f8 ff ff  leaq   -0x8(%rdx),%rdx'
dis_test "addq-->addq for SIB 2" func style1-with-r12 \
    'func+0x17: 49 81 c4 f0 ff ff  addq   $-0x10,%r12   <0xfffffffffffffff0>'

dis_test "movq-->movq" main style2 \
    'main+0x4:  48 c7 c6 f0 ff ff  movq   $-0x10,%rsi   <0xfffffffffffffff0>'

dis_test "movq-->movq w/REX" main style2-with-r13 \
    'main+0x4:  49 c7 c5 f0 ff ff  movq   $-0x10,%r13   <0xfffffffffffffff0>'
```



```
dis_test "movq-->movq incase of SIB" main style2-with-r12 \
    'main+0x4:  49 c7 c4 f0 ff ff  movq   $-0x10,%r12   <0xfffffffffffffff0>'

make -f ${TESTDIR}/Makefile.test fail TESTDIR=${TESTDIR} 2>&1 | grep_test "bad i
make PROTO="${1}" fail 2>&1 | grep_test "bad insn sequence" \
    'ld: fatal: relocation error: R_AMD64_TPOFF32: file style2-with-badness.o: sy
```

```
**********************************************************
     832 Thu Feb 28 22:40:49 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/style1-func-with-r12.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
______unchanged_portion_omitted_
```

```
**********************************************************
     925 Thu Feb 28 22:40:50 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/style2-with-badness.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
______unchanged_portion_omitted_
```

```
**********************************************************
     953 Thu Feb 28 22:40:51 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/style2-with-r12.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
   1 /*
   2  * This file and its contents are supplied under the terms of the
   3  * Common Development and Distribution License ("CDDL"), version 1.0.
   4  * You may only use this file in accordance with the terms of version
   5  * 1.0 of the CDDL.
   6  *
   7  * A full copy of the text of the CDDL should have accompanied this
   8  * source.  A copy of the CDDL is also available via the Internet at
   9  * http://www.illumos.org/license/CDDL.
  10  */

  12 /*
  13  * Copyright 2012, Richard Lowe.
  14  */

  16         .section        .rodata.str1.1,"aMS",@progbits,1
  17 .LC0:
  18         .string "foo: %p\n"
  19         .text
  20 .globl main
  21         .type   main, @function
  22 main:
  23 .LFB0:
  24         pushq   %rbp
  25 .LCFI0:
  26         movq    %rsp, %rbp
  27 .LCFI1:
  28         movq    foo@GOTTPOFF(%rip), %r12
  29         addq    %fs:0, %r12
  30         movq    %r12, %rsi
  31         movl    $.LC0, %edi
  32         movl    $0, %eax
  33         call    printf
  34         movl    $0, %eax
  35         leave
  36         ret
  37 .LFE0:
  38         .size   main, .-main
  39 .globl foo
  40         .section        .rodata.str1.1
  41 .LC1:
  42         .string "foo"

  44 #endif /* ! codereview */
  45         .section        .tdata,"awT",@progbits
  46         .align 8
  47         .type   foo, @object
  48         .size   foo, 8
  49 foo:
  50         .quad   .LC1
```

```
**********************************************************
     952 Thu Feb 28 22:40:51 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/style2-with-r13.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
______unchanged_portion_omitted_
```

```
**********************************************************
     925 Thu Feb 28 22:40:52 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ie/style2.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
______unchanged_portion_omitted_
```

```
**********************************************************
     974 Thu Feb 28 22:40:52 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ld/Makefile
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2018, Richard Lowe.

include $(SRC)/cmd/Makefile.cmd
include $(SRC)/test/Makefile.com

PROG =  amd64-ld-test

DATAFILES =             \
        Makefile.test   \
        ld-with-addend.s        \

ROOTOPTPKG = $(ROOT)/opt/elf-tests
TESTDIR = $(ROOTOPTPKG)/tests/tls/amd64/ld

CMDS = $(PROG:%=$(TESTDIR)/%)
$(CMDS) := FILEMODE = 0555


DATA = $(DATAFILES:%=$(TESTDIR)/%)
$(DATA) := FILEMODE = 0444

all: $(PROG)

install: all $(CMDS) $(DATA)

lint:

clobber: clean
        -$(RM) $(PROG)

clean:
        -$(RM) $(CLEANFILES)

$(CMDS): $(TESTDIR) $(PROG)

$(TESTDIR):
        $(INS.dir)

$(TESTDIR)/%: %
        $(INS.file)
#endif /* ! codereview */
```

****
813 Thu Feb 28 22:40:52 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ld/Makefile.test
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

CC =            gcc
CFLAGS =        -O1 -m64

LINK.c =  $(CC) $(CFLAGS) -o $@ $^
COMPILE.s = $(CC) $(CFLAGS) -c -o $@ $^

.KEEP_STATE:

install default: all

%.o: $(TESTDIR)/%.s
        $(COMPILE.s)

# an R_AMD64_DTPOFF32 with an addend, which must be preserved
PROGS +=        ld-with-addend

ld-with-addend: ld-with-addend.o
        $(LINK.c)

all:    $(PROGS)

clobber clean:
        rm -f $(PROGS) ld-with-addend.o

FRC:
#endif /* ! codereview */
```

```
**********************************************************
    1189 Thu Feb 28 22:40:53 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ld/amd64-ld-test.sh
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
**********************************************************
```

```
#!/bin/ksh
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

function grep_test {
    name=$1
    pattern=$2

    if /usr/bin/grep -q "${pattern}"; then
        print -u2 "pass: $name"
        else
        print -u2 "FAIL: $name"
        exit 1
    fi
}

function dis_test {
    name=${1}
    func=${2}
    file=${3}
    pattern=${4}

    dis -F${func} ${file} | grep_test "${name}" "${pattern}"
}

TESTDIR=$(dirname $0)

make -f ${TESTDIR}/Makefile.test TESTDIR=${TESTDIR}

# if we fail, the addend won't be applied, the leaq with be -0x10(%rax)
dis_test "addend is preserved" main ld-with-addend \
    'main+0x10: 48 8d b0 f2 ff ff  leaq   -0xe(%rax),%rsi'

# We have an addend of 2, a failure will print 'incorrect'
./ld-with-addend | grep_test 'ld-with-addend execution' \
    '^foo: correct ([a-f0-9]*)$'
#endif /* ! codereview */
```

****
936 Thu Feb 28 22:40:53 2019
new/usr/src/test/elf-tests/tests/tls/amd64/ld/ld-with-addend.s
10471 ld(1) amd64 LD->LE TLS transition causes memory corruption
****

```
/*
 * This file and its contents are supplied under the terms of the
 * Common Development and Distribution License ("CDDL"), version 1.0.
 * You may only use this file in accordance with the terms of version
 * 1.0 of the CDDL.
 *
 * A full copy of the text of the CDDL should have accompanied this
 * source.  A copy of the CDDL is also available via the Internet at
 * http://www.illumos.org/license/CDDL.
 */

/*
 * Copyright 2012, Richard Lowe.
 */

        .section        .rodata.str1.1,"aMS",@progbits,1
.LC0:
        .string "foo: %s (%p)\n"
        .text
        .section        .tdata,"awT",@progbits
foo:
        .string "incorrect"
        .text
.globl main
        .type   main, @function
main:
.LFB0:
        pushq   %rbp
.LCFI0:
        movq    %rsp, %rbp
        .LCFI1:
        leaq    foo@tlsld(%rip), %rdi
        call    __tls_get_addr@plt
        leaq    2+foo@dtpoff(%rax), %rsi
        movq    %rsi, %rdx
        movq    %rsi, %rsi
        movl    $.LC0, %edi
        movl    $0, %eax
        call    printf
        movl    $0, %eax
        leave
        ret
        .size   main, .-main
#endif /* ! codereview */
```

****
545 Thu Feb 28 22:40:53 2019
new/usr/src/test/elf-tests/tests/tls/i386/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

#
# Copyright (c) 2012, 2016 by Delphix. All rights reserved.
# Copyright 2018 Joyent, Inc.
#

SUBDIRS = ld

include $(SRC)/test/Makefile.com
#endif /* ! codereview */
```

```
**********************************************************
     966 Thu Feb 28 22:40:53 2019
new/usr/src/test/elf-tests/tests/tls/i386/ld/Makefile
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2018, Richard Lowe.

include $(SRC)/cmd/Makefile.cmd
include $(SRC)/test/Makefile.com

PROG =  i386-ld-test

DATAFILES =             \
        Makefile.test   \
        half-ldm.s      \

ROOTOPTPKG = $(ROOT)/opt/elf-tests
TESTDIR = $(ROOTOPTPKG)/tests/tls/i386/ld

CMDS = $(PROG:%=$(TESTDIR)/%)
$(CMDS) := FILEMODE = 0555


DATA = $(DATAFILES:%=$(TESTDIR)/%)
$(DATA) := FILEMODE = 0444

all: $(PROG)

install: all $(CMDS) $(DATA)

lint:

clobber: clean
        -$(RM) $(PROG)

clean:
        -$(RM) $(CLEANFILES)

$(CMDS): $(TESTDIR) $(PROG)

$(TESTDIR):
        $(INS.dir)

$(TESTDIR)/%: %
        $(INS.file)
#endif /* ! codereview */
```

****
797 Thu Feb 28 22:40:54 2019
new/usr/src/test/elf-tests/tests/tls/i386/ld/Makefile.test
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
****

```
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

CC =            gcc
CFLAGS =        -O1 -m32

LINK.c =  $(CC) $(CFLAGS) -o $@ $^
COMPILE.s = $(CC) $(CFLAGS) -c -o $@ $^

.KEEP_STATE:

install default: all

%.o: $(TESTDIR)/%.s
        $(COMPILE.s)

# an R_386_TLS_LDM with a regular R_386_PLT32 not a R_386_TLS_LDM_PLT
PROGS +=        half-ldm

half-ldm: half-ldm.o
        $(LINK.c)

all:    $(PROGS)

clobber clean:
        rm -f $(PROGS) half-ldm.o

FRC:
#endif /* ! codereview */
```

```
**********************************************************
    1355 Thu Feb 28 22:40:54 2019
new/usr/src/test/elf-tests/tests/tls/i386/ld/half-ldm.s
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
/*
 * This file and its contents are supplied under the terms of the
 * Common Development and Distribution License ("CDDL"), version 1.0.
 * You may only use this file in accordance with the terms of version
 * 1.0 of the CDDL.
 *
 * A full copy of the text of the CDDL should have accompanied this
 * source.  A copy of the CDDL is also available via the Internet at
 * http://www.illumos.org/license/CDDL.u
 */

/*
 * Copyright 2019, Richard Lowe.
 */

        .section .rodata.str1.1,"aMS",@progbits,1
.LC0:
        .string "foo: %s (%p)\n"
        .section .tdata,"awT",@progbits
        .align 4
        .type foo, @object
        .size foo,4
.local foo
foo:
        .string "foo"
        .text
.globl main
        .type main, @function
main:
        pushl %ebp
        movl %esp, %ebp
        /*
         * an R_386_TLS_LDM relocation without a following
         * followed by an R_386_PLT32 relocation, rather than an
         * R_386_TLS_LDM_PLT the call should be removed, and _not_
         * left alone unrelocated as it was prior to:
         * 10267 ld and GCC disagree about i386 local dynamic TLS
         */
        leal foo@TLSLDM(%ebx), %eax
        call ___tls_get_addr@PLT
        leal  foo@DTPOFF(%eax), %edx
        pushl %edx
        pushl %edx
        pushl $.LC0
        call printf@PLT
        movl $0x0,%eax
        leave
        ret
        .size main, .-main
#endif /* ! codereview */
```

```
**********************************************************
    1026 Thu Feb 28 22:40:54 2019
new/usr/src/test/elf-tests/tests/tls/i386/ld/i386-ld-test.sh
10367 ld(1) tests should be a real test suite
10368 want an ld(1) regression test for i386 LD tls transition (10267)
**********************************************************
```

```
#!/bin/ksh
#
# This file and its contents are supplied under the terms of the
# Common Development and Distribution License ("CDDL"), version 1.0.
# You may only use this file in accordance with the terms of version
# 1.0 of the CDDL.
#
# A full copy of the text of the CDDL should have accompanied this
# source.  A copy of the CDDL is also available via the Internet at
# http://www.illumos.org/license/CDDL.
#

# Copyright 2012, Richard Lowe.

function grep_test {
    name=$1
    pattern=$2

    if /usr/bin/grep -q "${pattern}"; then
        print -u2 "pass: $name"
        else
        print -u2 "FAIL: $name"
        exit 1
    fi
}

function dis_test {
    name=${1}
    func=${2}
    file=${3}
    pattern=${4}

    dis -F${func} ${file} | grep_test "${name}" "${pattern}"
}

TESTDIR=$(dirname $0)
make -f ${TESTDIR}/Makefile.test TESTDIR=${TESTDIR}

dis_test "call-->nop" main half-ldm \
    'main\+0x9:  0f 1f 44 00 00     nopl   0x0(%eax,%eax)'

./half-ldm | grep_test 'half-ldm execution' \
    '^foo: foo ([a-f0-9]*)$'
#endif /* ! codereview */
```