```
$kbyanc: dyntrace/patches/README,v 1.3 2004/12/23 01:45:20 kbyanc Exp $

This directory contains various patches to FreeBSD to implement new
functionality or fix existing bugs with regards to dynamic tracing
of processes.

All diffs are against FreeBSD 5.3.  Where noted, these patches have
been committed to FreeBSD's source repository to be included in future
releases.

trace-fix.diff
        Fixes a bug in the i386 machine-dependent portion of the fork(2)
        implementation in which the trap flag was copied from the parent
        to the child process.  This bug caused all children of processes
        being single-stepped under the control of a debugger to dump
        core immediately on return from the fork(2) call.  The cause was
        that the processor generates a SIGTRAP because the trap flag is
        set; the parent is under the control of a debugger which
        intercepts the signal so the parent never receives the it,
        however the new child is not and hence does receive the signal.
        The default signal handler for SIGTERM is to dump core.

        This patch simply clears the PSL_T (trace enable bit) in trap
        frame of the newly-created process.  It cannot possible be under
        the control of a debugger yet so it does not make sense to try
        to trace it (and, as witnessed, only ends in disaster).

        * Committed to FreeBSD src/sys/i386/i386/vm_machdep.c
          revision 1.247 (FreeBSD -current; for 6.0 release) 2004-12-08,
          revision 1.241.2.1 (FreeBSD RELENG_5; for 5.4 release) 2004-12-12
```

```
Index: vm_machdep.c
===================================================================
RCS file: /home/ncvs/src/sys/i386/i386/vm_machdep.c,v
retrieving revision 1.241
diff -u -p -r1.241 vm_machdep.c
--- vm_machdep.c        20 Jul 2004 01:38:59 -0000      1.241
+++ vm_machdep.c        1 Dec 2004 21:26:32 -0000
@@ -62,6 +62,7 @@ __FBSDID("$FreeBSD: src/sys/i386/i386/vm
 #include <sys/malloc.h>
 #include <sys/mbuf.h>
 #include <sys/mutex.h>
+#include <sys/pioctl.h>
 #include <sys/proc.h>
 #include <sys/sf_buf.h>
 #include <sys/smp.h>
@@ -201,6 +202,17 @@ cpu_fork(td1, p2, td2, flags)
        td2->td_frame->tf_edx = 1;

        /*
+        * If the parent process has the trap bit set (i.e. a debugger had
+        * single stepped the process to the system call), we need to clear
+        * the trap flag from the new frame unless the debugger had set PF_FORK
+        * on the parent.  Otherwise, the child will receive a (likely
+        * unexpected) SIGTRAP when it executes the first instruction after
+        * returning  to userland.
+        */
+       if ((p1->p_pfsflags & PF_FORK) == 0)
+               td2->td_frame->tf_eflags &= ~PSL_T;
+
+       /*
         * Set registers for trampoline to user mode.  Leave space for the
         * return address on stack.  These are the kernel mode register values.
         */
```