

# [PATCH]kprobe handler discard user space trap

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-02/msg09864.html>

---

- *From:* "bibo,mao" <bibo.mao@xxxxxxxx>
  - *Date:* Tue, 28 Feb 2006 15:23:12 +0800
- 

Currently kprobe handler traps only happen in kernel space, so function kprobe\_exceptions\_notify should skip traps which happen in user space. This patch modifies this, and it is based on 2.6.16-rc4.

Signed-off-by: bibo mao <bibo.mao@xxxxxxxx>

```
diff -Nruap a/arch/i386/kernel/kprobes.c b/arch/i386/kernel/kprobes.c
--- a/arch/i386/kernel/kprobes.c 2006-02-25 17:08:52.000000000 +0800
+++ b/arch/i386/kernel/kprobes.c 2006-03-01 10:37:50.000000000 +0800
@@ -463,6 +463,9 @@ int __kprobes kprobe_exceptions_notify(s
struct die_args *args = (struct die_args *)data;
int ret = NOTIFY_DONE;

+ if (user_mode(args->regs))
+ return ret;
+
switch (val) {
case DIE_INT3:
if (kprobe_handler(args->regs))
diff -Nruap a/arch/ia64/kernel/kprobes.c b/arch/ia64/kernel/kprobes.c
--- a/arch/ia64/kernel/kprobes.c 2006-02-25 17:08:53.000000000 +0800
+++ b/arch/ia64/kernel/kprobes.c 2006-03-01 10:39:15.000000000 +0800
@@ -740,6 +740,9 @@ int __kprobes kprobe_exceptions_notify(s
struct die_args *args = (struct die_args *)data;
int ret = NOTIFY_DONE;

+ if (user_mode(args->regs))
+ return ret;
+
switch(val) {
case DIE_BREAK:
/* err is break number from ia64_bad_break() */
diff -Nruap a/arch/powerpc/kernel/kprobes.c b/arch/powerpc/kernel/kprobes.c
--- a/arch/powerpc/kernel/kprobes.c 2006-02-25 17:08:52.000000000 +0800
+++ b/arch/powerpc/kernel/kprobes.c 2006-03-01 10:39:53.000000000 +0800
@@ -397,6 +397,9 @@ int __kprobes kprobe_exceptions_notify(s
struct die_args *args = (struct die_args *)data;
int ret = NOTIFY_DONE;
```

[PATCH]kprobe handler discard user space trap

```
+ if (user_mode(args->regs))
+ return ret;
+
switch (val) {
case DIE_BPT:
if (kprobe_handler(args->regs))
diff -Nruap a/arch/sparc64/kernel/kprobes.c b/arch/sparc64/kernel/kprobes.c
---- a/arch/sparc64/kernel/kprobes.c 2006-02-25 17:08:52.000000000 +0800
+++ b/arch/sparc64/kernel/kprobes.c 2006-03-01 10:40:16.000000000 +0800
@@ -324,6 +324,9 @@ int __kprobes kprobe_exceptions_notify(s
struct die_args *args = (struct die_args *)data;
int ret = NOTIFY_DONE;

+ if (user_mode(args->regs))
+ return ret;
+
switch (val) {
case DIE_DEBUG:
if (kprobe_handler(args->regs))
diff -Nruap a/arch/x86_64/kernel/kprobes.c b/arch/x86_64/kernel/kprobes.c
---- a/arch/x86_64/kernel/kprobes.c 2006-02-25 17:08:52.000000000 +0800
+++ b/arch/x86_64/kernel/kprobes.c 2006-03-01 10:38:48.000000000 +0800
@@ -601,6 +601,9 @@ int __kprobes kprobe_exceptions_notify(s
struct die_args *args = (struct die_args *)data;
int ret = NOTIFY_DONE;

+ if (user_mode(args->regs))
+ return ret;
+
switch (val) {
case DIE_INT3:
if (kprobe_handler(args->regs))
```

-  
To unsubscribe from this list: send the line "unsubscribe linux-kernel" in  
the body of a message to majordomo@xxxxxxxxxxxxxxxxxxx  
More majordomo info at <http://vger.kernel.org/majordomo-info.html>  
Please read the FAQ at <http://www.tux.org/lkml/>