

---

Subject: [PATCH] return correct error code from child\_rip in x86\_64 entry.S

Posted by [Andrey Mirkin](#) on Wed, 19 Sep 2007 14:26:25 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

From: Andrey Mirkin <major@openvz.org>

Right now register edi is just cleared before calling do\_exit.  
That is wrong because correct return value will be ignored.  
Value from rax should be copied to rdi instead of clearing edi.

Signed-off-by: Andrey Mirkin <major@openvz.org>

-----

```
diff --git a/arch/x86_64/kernel/entry.S b/arch/x86_64/kernel/entry.S
index 1d232e5..ac6400e 100644
--- a/arch/x86_64/kernel/entry.S
+++ b/arch/x86_64/kernel/entry.S
@@ -989,7 +989,7 @@ child_rip:
     movq %rsi, %rdi
     call *%rax
     # exit
-    xorl %edi, %edi
+    movq %rax, %rdi
     call do_exit
     CFI_ENDPROC
     ENDPROC(child_rip)
```

---