Subject: [PATCH] Sync compat getdents on ia64 and parisc
Posted by adobriyan on Wed, 21 Feb 2007 15:10:50 GMT
View Forum Message <> Reply to Message

From: Alexandr Andreev <aandreev@openvz.org>

Add VERIFY_WRITE check in the beginning like compat_sys_getdents()
[EINVAL vs EFAULT on ia64.
 EFAULT on parisc if put_user() fails. --adobriyan]

Can arch maintainers look if compat_sys_getdents() is OK for them?

Signed-off-by: Alexandr Andreev <aandreev@openvz.org>
Signed-off-by: Alexey Dobriyan <adobriyan@openvz.org>
---

 arch/ia64/ia32/sys_ia32.c | 10 +++++++---
 arch/parisc/kernel/sys_parisc32.c | 10 +++++++--
 2 files changed, 15 insertions(+), 5 deletions(-)

```
--- a/arch/ia64/ia32/sys_ia32.c
+++ b/arch/ia64/ia32/sys_ia32.c
@@ -1267,6 +1267,10 @@ sys32_getdents (unsigned int fd, struct
  struct getdents32_callback buf;
  int error;

+ error = -EFAULT;
+ if (!access_ok(VERIFY_WRITE, dirent, count))
+  goto out;
+
  error = -EBADF;
  file = fget(fd);
  if (!file)
@@ -1283,10 +1287,10 @@ sys32_getdents (unsigned int fd, struct
  error = buf.error;
  lastdirent = buf.previous;
  if (lastdirent) {
-  error = -EINVAL;
   if (put_user(file->f_pos, &lastdirent->d_off))
-   goto out_putf;
-  error = count - buf.count;
+   error = -EFAULT;
+  else
+   error = count - buf.count;
  }

 out_putf:
--- a/arch/parisc/kernel/sys_parisc32.c
```

```
+++ b/arch/parisc/kernel/sys_parisc32.c
@@ -350,6 +350,10 @@ sys32_getdents (unsigned int fd, void __
  struct getdents32_callback buf;
  int error;

+ error = -EFAULT;
+ if (!access_ok(VERIFY_WRITE, dirent, count))
+  goto out;
+
  error = -EBADF;
  file = fget(fd);
  if (!file)
@@ -366,8 +370,10 @@ sys32_getdents (unsigned int fd, void __
  error = buf.error;
  lastdirent = buf.previous;
  if (lastdirent) {
-  put_user(file->f_pos, &lastdirent->d_off);
-  error = count - buf.count;
+  if (put_user(file->f_pos, &lastdirent->d_off))
+   error = -EFAULT;
+  else
+   error = count - buf.count;
  }

 out_putf:
```