

[PATCH] [2.6.2-rc3] Fix module.c pointer arithmetics

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-01/7885.html>

From: Carl-Daniel Hailfinger (*c-d.hailfinger.kernel.2004_at_gmx.net*)

Date: 01/31/04

Date: Sat, 31 Jan 2004 13:52:48 +0100
To: Linus Torvalds <torvalds@osdl.org>

Linus,
Rusty,

while studying the module code closely, I found a problem in kernel/module.c:153ff.

```
for (i = 0; __start__ksymtab+i < __stop__ksymtab; i++)
```

In combination with `__start__ksymtab[i].name` this will go eight times too far. Proposed fix is attached.

Please apply before 2.6.2. If you think this makes the code too slow, I can offer an alternative which will even speed up the current code.

Thanks,
Carl-Daniel

```
===== kernel/module.c 1.99 vs edited =====
--- 1.99/kernel/module.c Wed Jan 21 02:50:58 2004
+++ edited/kernel/module.c Sat Jan 31 13:50:47 2004
@@ -150,14 +150,14 @@
```

```
    /* Core kernel first. */
    *owner = NULL;
- for (i = 0; __start__ksymtab+i < __stop__ksymtab; i++) {
+ for (i = 0; __start__ksymtab+i*sizeof(struct kernel_symbol) < __stop__ksymtab; i++) {
    if (strcmp(__start__ksymtab[i].name, name) == 0) {
        *crc = symversion(__start__krctab, i);
        return __start__ksymtab[i].value;
    }
}
if (gplok) {
```

Linux-Kernel: [PATCH] [2.6.2-rc3] Fix module.c pointer arithmetics

```
- for (i = 0; __start__ksymtab_gpl+i<__stop__ksymtab_gpl; i++)
+ for (i = 0; __start__ksymtab_gpl+i*sizeof(struct kernel_symbol) < __stop__ksymtab_gpl; i++)
    if (strcmp(__start__ksymtab_gpl[i].name, name) == 0) {
        *crc = symversion(__start__kcrctab_gpl, i);
        return __start__ksymtab_gpl[i].value;
@@ -1308,7 +1308,7 @@
    unsigned int i;

    if (!mod) {
- for (i = 0; __start__ksymtab+i < __stop__ksymtab; i++)
+ for (i = 0; __start__ksymtab+i*sizeof(struct kernel_symbol) < __stop__ksymtab; i++)
        if (strcmp(__start__ksymtab[i].name, name) == 0)
            return 1;
    return 0;

-
```

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