Subject: Re: [PATCH] IA64,sparc: local DoS with corrupted ELFs
Posted by fernando on Wed, 06 Sep 2006 23:23:11 GMT
View Forum Message <> Reply to Message

On Wed, 2006-09-06 at 13:20 -0700, Linus Torvalds wrote:
>
> On Mon, 4 Sep 2006, Kirill Korotaev wrote:
> >
> > +#ifdef __KERNEL__
> > +#define arch_mmap_check ia64_mmap_check
> > +#ifndef __ASSEMBLY__
> > +int ia64_mmap_check(unsigned long addr, unsigned long len,
> > + unsigned long flags);
> > +#endif
> > +#endif
>
> Btw, is there some reason for the __ASSEMBLY__ check?
>
> I'm not seeing any kernel users that could care, a quick
>
> git grep 'mman\.h' -- '*.[sS]'
>
> doesn't trigger anything, and the other header files that include this
> seem to all either be mman.h themselves, or have things like structure
> declarations etc that wouldn't work for any non-C source anyway.
>
> But maybe I missed some.
>
> I'd rather not have more of those '#ifndef __ASSEMBLY__' than necessary

The problem is that "asm/mman.h" is being included from entry.S indirectly
through "asm/pgtable.h" (see code snips below).

* arch/ia64/kernel/entry.S:
...
#include <asm/pgtable.h>
...

* include/asm-ia64/pgtable.h:
...
#include <asm/mman.h>
...

* include/asm-ia64/mman.h
...
#ifdef __KERNEL__
#define arch_mmap_check ia64_map_check_rgn
int ia64_map_check_rgn(unsigned long addr, unsigned long len,

```
            unsigned long flags);
#endif
...
```

Without this fix compilation is broken:

```
  gcc -Wp,-MD,arch/ia64/kernel/.entry.o.d  -nostdinc -isystem
/usr/lib/gcc/ia64-linux-gnu/4.1.2/include -D__KERNEL__ -Iinclude  -include
include/linux/autoconf.h -DHAVE_WORKING_TEXT_ALIGN
-DHAVE_MODEL_SMALL_ATTRIBUTE -DHAVE_SERIALIZE_DIRECTIVE -D__ASSEMBLY__
-mconstant-gp -c -o arch/ia64/kernel/entry.o arch/ia64/kernel/entry.S
include/asm/mman.h: Assembler messages:
include/asm/mman.h:13: Error: Unknown opcode `int ia64_map_check_rgn(unsigned long
addr,unsigned long len,'
include/asm/mman.h:14: Error: Unknown opcode `unsigned long flags)'
make[1]: *** [arch/ia64/kernel/entry.o] Error 1
make: *** [arch/ia64/kernel] Error 2
```

Regards,

Fernando