
Subject: Re: [PATCH] IA64,sparc: local DoS with corrupted ELF's

Posted by [dev](#) on Tue, 05 Sep 2006 13:06:57 GMT

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

Andrew, Kyle,

> On Mon, Sep 04, 2006 at 04:17:00PM +0400, Kirill Korotaev wrote:

>

>>--- a/include/asm-generic/mman.h

>>+++ b/include/asm-generic/mman.h

>>@@ -39,4 +39,10 @@ #define MADV_DOFORK 11 /* do inherit ac

>>#define MAP_ANON MAP_ANONYMOUS

>>#define MAP_FILE 0

>>

>>+#ifdef __KERNEL__

>>+#ifndef arch_mmap_check

>>+#define arch_mmap_check(addr, len, flags) (0)

>>+#endif

>>+#endif

>>+

>>#endif

>

>

> This breaks all arches that don't use asm-generic/mman.h, and that you

> didn't add arch_mmap_check to asm/mman.h for.

oops... You are right.

is define

#define arch_mmap_check(addr, len, flags) (0)

ok for you in such mman.h headers which do not include asm-generic/mman.h?

If yes, the following patch should help.

Though I didn't get the idea of include/asm-um/mman.h:

#include "asm/arch/mman.h"

This patch adds define of arch_mmap_check() to

archs which do not include include/asm-generic/mman.h

diff --git a/include/asm-alpha/mman.h b/include/asm-alpha/mman.h

index 5f24c75..51cf354 100644

--- a/include/asm-alpha/mman.h

+++ b/include/asm-alpha/mman.h

@@ -52,4 +52,10 @@ #define MADV_DOFORK 11 /* do inherit ac

#define MAP_ANON MAP_ANONYMOUS

#define MAP_FILE 0

```

+msgid __KERNEL__
+msgid arch_mmap_check
+#define arch_mmap_check(addr, len, flags) (0)
+#endif
+
+
+endif /* __ALPHA_MMAN_H__ */
diff --git a/include/asm-mips/mman.h b/include/asm-mips/mman.h
index 046cf68..f19e858 100644
--- a/include/asm-mips/mman.h
+++ b/include/asm-mips/mman.h
@@ -75,4 +75,10 @@ #define MADV_DOFORK 11 /* do inherit ac
#define MAP_ANON MAP_ANONYMOUS
#define MAP_FILE 0

+msgid __KERNEL__
+msgid arch_mmap_check
+#define arch_mmap_check(addr, len, flags) (0)
+#endif
+
+
+endif /* _ASM_MMAN_H */
diff --git a/include/asm-parisc/mman.h b/include/asm-parisc/mman.h
index 0ef15ee..9829b31 100644
--- a/include/asm-parisc/mman.h
+++ b/include/asm-parisc/mman.h
@@ -59,4 +59,10 @@ #define MAP_ANON MAP_ANONYMOUS
#define MAP_FILE 0
#define MAP_VARIABLE 0

+msgid __KERNEL__
+msgid arch_mmap_check
+#define arch_mmap_check(addr, len, flags) (0)
+#endif
+
+
+endif /* __PARISC_MMAN_H__ */

```
