Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Tue, 12 Feb 2008 00:15:54 GMT
View Forum Message <> Reply to Message

I can confirm, what at least one exploit does not work

```
 Linux vmsplice Local Root Exploit
 By qaaz
---------------------------------
[+] mmap: 0x100000000000 .. 0x100000001000
[+] page: 0x100000000000
[+] page: 0x100000000038
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4038
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0x2aaaaaab9000 .. 0x2aaaaaaeb000
[-] vmsplice: Bad address
```

after patch from src.rpm (http://erek.blumenthals.com/blog/2008/02/11/rhel-5-centos-5-kernel-rpms-patched-against-vmsplice-local-root-exploit/):

```
--- a/fs/splice.c
+++ b/fs/splice.c
@@ -1234,7 +1234,7 @@ static int get_iovec_page_array(const struct iovec __user *iov,
                if (unlikely(!len))
                        break;
                error = -EFAULT;
-               if (unlikely(!base))
+               if (!access_ok(VERIFY_READ, base, len))
                        break;

                /*
```

Another sploit does not compile on x86_64 with next error
: "Error: Incorrect register `%rax' used with `l' suffix"

So I just realy don't know.

And, as I understand, very soon RedHat will release their solution. After Qa tests.

https://bugzilla.redhat.com/show_bug.cgi?id=432251