
Subject: Re: kernel exploit in the wild

Posted by [Steve Wray](#) on Mon, 11 Feb 2008 01:56:52 GMT

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

John Maclean wrote:

> There's a kernel exploit in the wild [0]. I've run it on a couple of
> nodes and it __does__ allow a non-root user root access. Has any one
> tried it on a Hardware node or within a VE? Within a VE all I got was a
> kernel oops and it was too low-level for me to decypher...
>
> [0] https://bugzilla.redhat.com/show_bug.cgi?id=432229

I tried it.

On a VE it gives a segfault

./a.out

```
-----  
Linux vmsplice Local Root Exploit  
By qaaz  
-----
```

```
[+] mmap: 0x0 .. 0x1000  
[+] page: 0x0  
[+] page: 0x20  
[+] mmap: 0x4000 .. 0x5000  
[+] page: 0x4000  
[+] page: 0x4020  
[+] mmap: 0x1000 .. 0x2000  
[+] page: 0x1000  
[+] mmap: 0xb7e37000 .. 0xb7e69000  
Segmentation fault
```

If you go and have a look at the host theres an oops:

BUG: unable to handle kernel NULL pointer dereference at virtual address
00000000

The system becomes unstable after this.
