Subject: Kernel Exploit, affect OpenVZ?
Posted by duswil on Sun, 10 Feb 2008 22:43:05 GMT
View Forum Message <> Reply to Message

http://it.slashdot.org/article.pl?sid=08/02/10/2011257

Kernel exploit that allows for privilege escalation.

Does this affect anyone on OpenVZ kernels? I tried it on a few of my test machines and they all failed to get root. They segfaulted before anything seemed to even happen.

Anyone have this work successfully on their OpenVZ servers?

Thanks,
Dusty

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by duswil on Sun, 10 Feb 2008 22:47:42 GMT
View Forum Message <> Reply to Message

On a test machine:

```
testuser@testvps1:~$ ./exploit
---------------------------------
 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: 0xb7e60000 .. 0xb7e92000
Segmentation fault
testuser@testvps1:~$
Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: Oops: 0000 [#2]

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: SMP

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: CPU:    1, VCPU: 3001.1
```

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: EIP is at 0x1fff

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: eax: 00000040 ebx: 00000004 ecx: 00000001 edx: 00004000

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: esi: d11a5f90 edi: ffffffe0 ebp: 00000001 esp: d11a5e94

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: ds: 007b es: 007b ss: 0068

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: Process exploit (pid: 29198, veid: 3001, ti=d11a4000 task=ed59d2a0 task.ti=d11a4000)

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: Stack: c014d327 c0182dd5 00000000 00000000 00000000 00000000 00000030 00000030

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: c01839ae d11a6010 d6f92da0 ec469e00 00000030 00000000 00000001 00000000

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: 00001000 00000000 00001000 00000000 00001000 00000000 00001000 00000000

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: Code: Bad EIP value.

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: EIP: [<00001fff>] 0x1fff SS:ESP 0068:d11a5e94

Message from syslogd@testbox at Sun Feb 10 22:45:18 2008 ...
testbox kernel: Call Trace:

testuser@testvps1:~$

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Avi Brender on Sun, 10 Feb 2008 23:39:11 GMT
View Forum Message <> Reply to Message

Hi,

We are seeing the same thing - segfaults but no escalation.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by blueboxgroup on Mon, 11 Feb 2008 04:53:05 GMT
View Forum Message <> Reply to Message

In our internal testing it appears to totally hang a machine with a Segfault when running inside a Debian VPS. Ubuntu appears fine.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Mon, 11 Feb 2008 09:41:13 GMT
View Forum Message <> Reply to Message

After reworking on sploit, as I think, it could be used for priv. esc. Need to use hotfix

http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6
.git;a=blobdiff;f=fs/splice.c;h=14e2262c0a046641ece8086c7f73
29a8a114ebda;hp=4ee49e86edde5a2272781b6e49e0371b721ceb33;hb=
8811930dc74a503415b35c4a79d14fb0b408a361;hpb=66191dc622f5ff0
a541524c4e96fdacfacfda206

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Avi Brender on Mon, 11 Feb 2008 14:53:48 GMT
View Forum Message <> Reply to Message

Actually, if we run the exploit multiple times in rapid succession we found that important processes (sshd etc) were segfaulting and required the machine to be rebooted. Can anyone else confirm that?

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Mon, 11 Feb 2008 15:05:56 GMT
View Forum Message <> Reply to Message

I can confirm it on latest 2.6.18 openvz kernel in hardware node. In vps I'll check later, but I'll think result will be the same. As I understand, ddos is more simple effect from this sploit. Priv. esc. is harder, but where is confrims from centos 5 (def installation) users, what it's works on i386 arch. On x86_64 and powerpc etc sploit need to be changed. So all should upgrade.

From Centos bugzilla i'll know - they waiting upstream RedHat fix or kernel package. In vanilla git fix is already made.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Avi Brender on Mon, 11 Feb 2008 17:40:58 GMT
View Forum Message <> Reply to Message

Hi,

To clarify, you can confirm the dos but not the priv escalation, correct?

For 32 bit architectures, this module http://home.powertech.no/oystein/ptpatch2008/ will protect you until a fix is released.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Mon, 11 Feb 2008 18:44:13 GMT
View Forum Message <> Reply to Message

//Sorry for english.

Well, right now I can check it only on x86_64. Because it's near me. In HN, after first try - it is die. On i386 I don't want check - it is far away from me.

About this module. I have seen message in some bugzilla (don't remember which, redhat or debian or gentoo), where exploit has been working after installing and loading module. I prefer to look on patch from git and try apply it to openvz kernel. Also, I think, in bugzilla's already can be new info by this day. So it will be good re-check it.

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

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Tue, 12 Feb 2008 08:41:51 GMT
View Forum Message <> Reply to Message

Please, also look here:
https://bugzilla.redhat.com/show_bug.cgi?id=432229
There is another temporary solution. Use systemtap to block this syscall. kernel-debuginfo must be installed to get work it.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Valmont on Tue, 12 Feb 2008 23:15:35 GMT
View Forum Message <> Reply to Message

So, RedHat had created necessary update:
ftp://ftp.redhat.com/pub/redhat/linux/enterprise/5Server/en/os/SRPMS/kernel-2.6.18-53.1.13.el5.src.rpm

You can take official patch from there or wait until new OpenVZ kernel release. It's depends on how urgent this problem for your server.

Subject: Re: Kernel Exploit, affect OpenVZ?
Posted by Avi Brender on Wed, 13 Feb 2008 17:16:31 GMT
View Forum Message <> Reply to Message

Any word on when we can expect an OpenVZ release?