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:~$