Subject: Kernel Root Exploit?
Posted by mperkel on Mon, 11 Feb 2008 18:08:52 GMT
View Forum Message <> Reply to Message

Someone alerted me to this.

https://bugzilla.redhat.com/show_bug.cgi?id=432229

Description of problem:

Local user can obtain root access (as described below).

This bug is being actively exploited in the wild -- our server was just broken
in to by an attacker using it. (They got a user's password by previously
compromising a machine somewhere else where that user had an account, and
installed a modified ssh binary on it to record user names and passwords. Then
they logged in to our site as that user, exploited CVE-2008-0010, and became root).

It is EXTREMELY urgent that a fixed kernel be provided ASAP given that this bug
is being actively exploited in the wild.

There is a fix listed upstream in 2.6.23.15 and 2.6.24.1. However, even after
applying that patch and recompiling the kernel, the escalation-of-privilege
exploit still worked so I am wondering if 2.6.23.15 does not completely fix it.

Version-Release number of selected component (if applicable):

All 2.6.23.x kernels

How reproducible: 100%

Steps to Reproduce:
1. Download http://downloads.securityfocus.com/vulnerabilities/exploits/ 27704.c
2. cc -o exploit 27704.c
3. [as non-privileged user] ./exploit

Actual results:

Root shell

Expected results:

No root shell.

Additional info:

When I altered the kernel spec file for 2.6.23.14-115.fc8 to pull 2.6.23.15
instead of 2.6.23.14 (and altered linux-2.6-highres-timers.patch to apply

cleanly, and removed the already-included-in-2.6.23.15 patches linux-2.6-net-silence-noisy-printks.patch and linux-2.6-freezer-fix-apm-emulation-breakage.patch), rebuilt a new kernel RPM, installed it, and rebooted, the above exploit still worked. So it is possible an additional patch is needed against 2.6.23, unless I just goofed somehow in my kernel rebuild. (I did check and the file fs/splice.c was correctly patched and included the lines that were suppose to fix this problem...)

More info:

Marc,

Even better:

http://home.powertech.no/oystein/ptpatch2008/

Subject: Re: Kernel Root Exploit?
Posted by xemul on Wed, 13 Feb 2008 10:03:23 GMT
View Forum Message <> Reply to Message

http://bugzilla.openvz.org/show_bug.cgi?id=814

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 11:43:50 GMT
View Forum Message <> Reply to Message

i tried the exploit in my enviroment and it didn't work thanks GOD

ls1614 kernel: Process exploit (pid: 21070, veid: 0, ti=d2e3c000 task=ea49cdf0 task.ti=d2e3c000)

however i didn't even update or patch my kernel

uname -a
Linux ssss.sssssss.net 2.6.18-ovz028stab023.1-smp #1 SMP Tue Mar 20 17:39:04 MSK 2007 i686 i686 i386 GNU/Linux

---

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 11:51:03 GMT
View Forum Message <> Reply to Message

sadly the whole server went offline few seconds later and it also sent an oops

---

Subject: Re: Kernel Root Exploit?
Posted by mperkel on Fri, 15 Feb 2008 13:09:10 GMT
View Forum Message <> Reply to Message

When my friend who alerted me to the problem tried it they not only gained root access but both time the Kernel did and oops a few hours later and crashed. But - that was with the stock fedora kernel, not OpenVZ.

Subject: Re: Kernel Root Exploit?
Posted by elronxenu on Fri, 15 Feb 2008 13:50:24 GMT
View Forum Message <> Reply to Message

I have posted a patch to the latest stable OpenVZ kernel here:

http://www.nick-andrew.net/Patches/20080213-openvz-2.6.18-st ab053-security.patch

Use at your own risk, YMMV etc. Apply by changing into the kernel top-level directory and running:

"patch -p0 < 20080213-openvz-2.6.18-stab053-security.patch".

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 14:01:24 GMT
View Forum Message <> Reply to Message

why not openvz release an urgent version of patched kernel instead of leaving all our servers to be hacked by lamers ????????

---

elronxenu thanks for your patch
could you please describe to me all details to have my kernel patched as i have never done this before

Subject: Re: Kernel Root Exploit?
Posted by mperkel on Fri, 15 Feb 2008 14:04:43 GMT
View Forum Message <> Reply to Message

I would have to second that. Fedora had a new kernel out the same day. And I need at 2.6.20+ kernel as I'm running Fedora 8 which requires that.

Subject: Re: Kernel Root Exploit?

Posted by sspt on Fri, 15 Feb 2008 14:26:24 GMT
View Forum Message <> Reply to Message

There are updates available for 2.6.18
http://download.openvz.org/kernel/branches/?C=M;O=D

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 14:38:24 GMT
View Forum Message <> Reply to Message

yes
i tried installing but i got the following warning

```
# rpm -ivh  http://download.openvz.org/kernel/branches/2.6.18/stable/ker
nel-smp-2.6.18-ovz028stab053.5.i686.rpm
Retrieving  http://download.openvz.org/kernel/branches/2.6.18/stable/ker
nel-smp-2.6.18-ovz028stab053.5.i686.rpm
Preparing...                ########################################### [100%]
   1:kernel-smp             ########################################### [100%]
WARNING: No module sata_sis found for kernel 2.6.18-ovz028stab053.5-smp, continuing anyway
```

is it safe to reboot using that new version of ovzkernel now ?

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 16:23:16 GMT
View Forum Message <> Reply to Message

hello
i rebooted to latest stable kernel
but the server keeps crashing every few minutes
nothing in top or /var/log/messages
it just gets offline

Subject: Re: Kernel Root Exploit?
Posted by sara3 on Fri, 15 Feb 2008 23:01:19 GMT
View Forum Message <> Reply to Message

strangest thing is happening
when i stopped a ve it made the hole server offline to me

no kernel oops or panic in the messages

load was ok at that time

did the network service die or its another problem ?
how to investiage and fix ?

Subject: Re: Kernel Root Exploit?
Posted by elronxenu on Sat, 16 Feb 2008 00:08:29 GMT
View Forum Message <> Reply to Message

My patch is against 2.6.18-028stab053.4 and there's now a .5 which presumably includes the fix so you can use that version instead.

My patch was for people who patch and configure the kernel themselves. The basic sequence of operations is:

1. Download and unpack original Linus kernel
2. Download and apply appropriate OpenVZ patch
3. Download and apply my patch
4. Configure and build kernel
5. Install kernel onto target hosts.

Subject: Re: Kernel Root Exploit?
Posted by mperkel on Sat, 16 Feb 2008 00:17:24 GMT
View Forum Message <> Reply to Message

I can't use any of these kernels because I'm running Fedora 8 and need a 2.6.20+ kernel.

Subject: Re: Kernel Root Exploit?
Posted by xemul on Mon, 18 Feb 2008 08:21:37 GMT
View Forum Message <> Reply to Message

2.6.20+ kernels are development ones. This means, that they are not as stable as 2.6.18 is and some of them (2.6.20 and 2.6.22) are no longer supported.

But why can't you use the 2.6.18 kernel? Are there any functionality missed or API changed? Please report and we'll try to solve these issues.
