Subject: Linux kernel null pointer bug
Posted by bucasia on Mon, 17 Aug 2009 11:13:08 GMT
View Forum Message <> Reply to Message

Does anyone know how the OpenVZ kernel is affected by this bug - http://www.securityfocus.com/bid/36038/info ? Thanks.

edit: I guess I should be a little more specific -

Does it give VPS containers access to the main node?
Will a patched kernel be issued - specifically for CentOS?

Thanks again!

Subject: Re: Linux kernel null pointer bug
Posted by khorenko on Tue, 18 Aug 2009 12:35:58 GMT
View Forum Message <> Reply to Message

Hi.

2.6.18-128.2.1.el5.028stab064.4 kernel (latest stable OVZ) is immune to the exploits on the issue.

The kernel is immune due to the fact that 64.4 kernel has the bypassing "mmap_min_addr" issue fixed:
http://blog.cr0.org/2009/06/bypassing-linux-null-pointer.htm l - description of the problem

Exploits for the current issue, in their turn, need this hole to gain root access.

--
Konstantin

Subject: Re: Linux kernel null pointer bug
Posted by bucasia on Tue, 18 Aug 2009 12:42:51 GMT
View Forum Message <> Reply to Message

Hi Konstantin,

That's good news. Thanks for taking the time to update this thread.

Matt

Subject: Re: Linux kernel null pointer bug
Posted by lazy on Tue, 25 Aug 2009 19:20:02 GMT

View Forum Message <> Reply to Message

finist wrote on Tue, 18 August 2009 08:35Hi.

2.6.18-128.2.1.el5.028stab064.4 kernel (latest stable OVZ) is immune to the exploits on the issue.

The kernel is immune due to the fact that 64.4 kernel has the bypassing "mmap_min_addr" issue fixed:
http://blog.cr0.org/2009/06/bypassing-linux-null-pointer.htm l - description of the problem

Exploits for the current issue, in their turn, need this hole to gain root access.

but still it's possible to destabilize the kernel with a failed exploit attempt

and there is another bug fixed in RHSA-2009:1222-02
https://rhn.redhat.com/errata/RHSA-2009-1222.html
bug
https://bugzilla.redhat.com/show_bug.cgi?id=518034

tonight i'm rolling 64.4 with patches from upstream
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6
.git;a=commitdiff;h=1e0c14f49d6b393179f423abbac47f85618d3d46

testing went threw ok, i will se if there will be any problems in production

Subject: Re: Linux kernel null pointer bug
Posted by khorenko on Wed, 26 Aug 2009 06:54:41 GMT
View Forum Message <> Reply to Message

Quote:but still it's possible to destabilize the kernel with a failed exploit attempt

Not exactly: you need to modify exploit to do this. But yes, it's possible, but again - from Hardware Node only.

Quote:and there is another bug fixed in RHSA-2009:1222-02
https://rhn.redhat.com/errata/RHSA-2009-1222.html
...
testing went threw ok, i will se if there will be any problems in production

Yes, we've already seen that, thank you.

--
Konstantin

Subject: Re: Linux kernel null pointer bug
Posted by lazy on Wed, 26 Aug 2009 07:17:25 GMT
View Forum Message <> Reply to Message

finist wrote on Wed, 26 August 2009 02:54Quote:but still it's possible to destabilize the kernel with a failed exploit attempt

Not exactly: you need to modify exploit to do this. But yes, it's possible, but again - from Hardware Node only.

Quote:and there is another bug fixed in RHSA-2009:1222-02
https://rhn.redhat.com/errata/RHSA-2009-1222.html
...
testing went threw ok, i will se if there will be any problems in production

Yes, we've already seen that, thank you.

I recall when when I started one of the exploits from 32 bit guest(64 bit host), its process got blocked in kernel space and I couldn't enter any other vps, reboot machine properly etc.
when I have some time I will recheck it (maybe after all I wasn't running 64.4 on that machine)
exploit was modified to run without kernel symbols in /proc

patched machines are working fine, is applying mentioned patch is sufficient ? (debian is using this patch for etch kernel so i guess it's safe to think so)

thanks for Your answer
--
Lazy