Subject: Kernel panic
Posted by lorenzo_3 on Thu, 13 Nov 2008 17:06:29 GMT
View Forum Message <> Reply to Message

Hi there,

I'm currently working for a webhoster, and we would like to integrate openvz in our networking arch.

We also would like to offers containers, for people who want ssh access.
My problem is that if someone exploit a local kernel panic exploit inside a Vz container, the whole box and all containers gets knocked out.
If our boxes, are located in a D.C, we wont be able to reboot it, until the D.C admin reboot manually the boxes.
This is actually a very big problem for us as security matter, and i would like to know if there's a way to solve this problem.

Thanks you for your time.

Regards

Subject: Re: Kernel panic
Posted by khorenko on Thu, 13 Nov 2008 17:44:38 GMT
View Forum Message <> Reply to Message

Hello,

well, yes, as all Containers are running under one kernel on a Hardware Node, if someone trigger a kernel panic, all the Containers on this node will be affected. This is a "minus".

* but in fact not all exploits will work inside a Container, and this is a "plus".
* next thing - not in all cases you'll have to wait for a manual reboot:

- first and the most useful in the current situation: you can add "panic=N" kernel option to the bootloader config and the kernel will reboot the node automatically after "N" seconds after it got a panic. This option really works in the 99% cases when you get an oops.
- second: you can ask D.C to configure remote power control - simplest PDU or more intelligent separate card inserted to the server if possible - quite a widespread feature nowadays.

BTW, can you please share your experience - how many oopses due to exploits have you got for some period of time? (+ how many nodes there were total and how often did you upgrade kernels on them).

Thank you!

--
Konstantin

Subject: Re: Kernel panic
Posted by lorenzo_3 on Thu, 13 Nov 2008 18:01:39 GMT
View Forum Message <> Reply to Message

finist wrote on Thu, 13 November 2008 12:44Hello,
BTW, can you please share your experience - how many oopses due to exploits have you got for some period of time? (+ how many nodes there were total and how often did you upgrade kernels on them).

Thank you!

Thanks you very much for your fast answer, the exploit is public
and there's actually no patch for the moment (hxxp://www.securityfocus.com/bid/32154)
This exploit call a panic instantly, and no login is done in dmesg/syslog/messages on the container and on the
main box.

Regards

Subject: Re: Kernel panic
Posted by kir on Thu, 13 Nov 2008 19:22:17 GMT
View Forum Message <> Reply to Message

So, have you tried running it inside an OpenVZ container? What are your results? Which kernels are affected and which are not?

Subject: Re: Kernel panic
Posted by lorenzo_3 on Thu, 13 Nov 2008 19:39:57 GMT
View Forum Message <> Reply to Message

kir wrote on Thu, 13 November 2008 14:22So, have you tried running it inside an OpenVZ container? What are your results?

Yes, and the whole box get smashed in less than a second, plus you need to reboot manually the box.

Quote:Which kernels are affected and which are not?

For the moment all, according to securityfocus, you can see it by clicking the link i've submitted in my previous post.

Also i tryed this exploit on 2 openvz kernel version :
-2.6.18
-2.6.24

And on a normal ubuntu box fully updated
2.6.27-7

Regards

Subject: Re: Kernel panic
Posted by khorenko on Fri, 14 Nov 2008 06:29:28 GMT
View Forum Message <> Reply to Message

Quote:Thanks you very much for your fast answer, the exploit is public
and there's actually no patch for the moment

https://bugzilla.redhat.com/show_bug.cgi?id=470201

We're working on fixing that.

--
Konstantin