
Subject: CentOS vulnerabilities detected by Nessus
Posted by [fvafva](#) on Thu, 14 Jun 2018 11:58:09 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

We are using different versions of openVZ on top of CentOS 6.

Nessus scanner is detecting for example :
The remote host is running Linux Kernel 2.6.32-042stab128.2 on CentOS release 6.9 (Final)

But is reporting the following :
Remote package installed : kernel-2.6.32-696.el6
Should be : kernel-2.6.32-696.6.3.el6

Because it is checking the CentOS version.

My question (I am not familiar enough with openVZ):
stab128, stab129, stab130 ... are all based on different CentOS kernels?
Do we have to consider CentOS vulnerabilities, like Nessus is doing?

Thanks for your answers.

Subject: Re: CentOS vulnerabilities detected by Nessus
Posted by [vaverin](#) on Fri, 15 Jun 2018 08:57:02 GMT
[View Forum Message](#) <> [Reply to Message](#)

Dear fvafva,

Our kernels are based on last released RHEL6 kernels.

We are monitoring public security mailing lists,
timely detect issues critical for containers,
and timely release fixed kernels.

Take a look:
openVZ6 kernel 042stab128.2 was released 26 March 2018 it is based on RHEL6 kernel 2.6.32-696.23.1.el6 released 13 March 2018.
Our next kernel 042stab129.1 was released 15 May 2018 and it is based on RHEL6 kernel 2.6.32-696.28.1.el6 released 8 May 2018.
Our last kernel 042stab130.1 was released 23 May 2018 and it is based on last RHEL6 2.6.32-696.30.1.el6 released 21 May 2018.

Moreover our kernels includes many security fixes not included yet into RHEL kernels.

I do not know what is Nessus and how it works,
however anyway from security point of view our last released kernels at least are not worse than

last released RHEL kernels.

Thank you,
Vasily Averin

Subject: Re: CentOS vulnerabilities detected by Nessus
Posted by [fvafva](#) on Fri, 15 Jun 2018 09:48:22 GMT
[View Forum Message](#) <> [Reply to Message](#)

Thanks for your answer.

I agree you include sometimes security fixes that are not yet in RHEL, bravo!

But as Nessus is detecting the RHEL one, and not openVZ one, it is creating some confusion. For example, if I am using 042stab128.2, Nessus will tell me about vulnerabilities that are in 2.6.32-696.23.1.el6, even if you already fixed them in openVZ. I would say it is normal behavior, nothing to discuss about that.

But may I consider 042stab128.2 secure? Probably not, as it is not the last version, and 042stab130.1 contains new security fixes. So every time Nessus is reporting an issue with CentOS version, that probably means I am not up-to-date on openVZ side.

Anyway, thanks for your answer.
