Subject: Re: kernel security issue on RHEL5 x86_64
Posted by canfone on Mon, 20 Sep 2010 18:17:58 GMT
View Forum Message <> Reply to Message

There is a new kernel security issue out:

https://access.redhat.com/kb/docs/DOC-40265

http://www.webhostingtalk.com/showthread.php?t=981925

Does anyone know how this would affect OpenVZ kernel, can we expect an update to resolve this security issue soon?

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by pug123 on Tue, 21 Sep 2010 08:45:13 GMT
View Forum Message <> Reply to Message

This is very serious issue. I wonder if attacker can gain access via VE into VPS node.

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by TheStig on Tue, 21 Sep 2010 09:43:37 GMT
View Forum Message <> Reply to Message

i've tested the exploit (http://sota.gen.nz/compat2/robert_you_suck.c) yesterday on two openvz-kernles 2.6.24-23-openvz (ubuntu 8.04) 2.6.26-2-openvz-amd64 (debian lenny) and it apparently didn't work ./robert_you_suck
symbol table not available, aborting!
Process finished

openvz is also mentioned in connection with this bug here:
http://seclists.org/fulldisclosure/2010/Sep/268

but i can't figure out what is meant by "OpenVZ Payload / GRsec bypass removed for kidiots and fame whores. (same thing right)
"

ps: i've tested the exploit on the HN not a VPS

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by matrix64 on Tue, 21 Sep 2010 10:23:32 GMT

View Forum Message <> Reply to Message

I've tested it on 2.6.32.15-openvz and it only works if you run it on HN. When I ran it in 32 or 64-bit VE it didn't work.

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by TheStig on Wed, 22 Sep 2010 14:11:27 GMT
View Forum Message <> Reply to Message

new 2.6.32 based kernel available
http://wiki.openvz.org/Download/kernel/2.6.32/2.6.32-dyomin. 1

i'm currently compiling for my openvz-testbed, as the ovz-2.6.32.14-kernel that is running atm is susceptible to the exploit.

BTW: http://bugzilla.openvz.org/show_bug.cgi?id=1542 is still _NOT_ fixed.

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by TheStig on Wed, 22 Sep 2010 16:03:38 GMT
View Forum Message <> Reply to Message

```
testuser@baghira:~$ ./robert_you_suck
resolved symbol commit_creds to 0xffffffff81075ad8
resolved symbol prepare_kernel_cred to 0xffffffff810759ef
mapping at 3f80000000
UID 519, EUID:519 GID:1000, EGID:1000
$ uname -r
2.6.32.22-ovz-dyomin.1
$ whoami
testuser
```

perfect ,-)

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by dabora on Thu, 11 Nov 2010 10:08:13 GMT
View Forum Message <> Reply to Message

If in RHEL 6 will include fresh packages, the need for Fedora can be reduced. Only RHEL 6 is wait and wait: the cycle of the release of RHEL - 3 years, and then the second version will not until the autumn.

Subject: Re: kernel security issue on RHEL5 x86_64
Posted by Ales on Fri, 12 Nov 2010 10:46:05 GMT

View Forum Message <> Reply to Message

I don't completely understand what you tried to say, but RHEL 6 was released two days ago. Finally!