Subject: Re: IMPORTANT: latest RHEL4 kernel has a root exploit!! (2.6.9-023stab016.2)
Posted by dev on Thu, 12 Oct 2006 09:49:00 GMT
View Forum Message <> Reply to Message

Dmitry has already uploaded a new kernel at
http://download.openvz.org/kernel/rhel4/023stab030.1/
Changelog and announce will be posted today as well.

next week we plan to fully switch to RHEL4 kernel for stable branch
and freeze our previous stable 2.6.8 branch.
After that RHEL4 kernels will be updated regularly without delays.

Thanks,
Kirill

Avi Brender wrote:
> Hi,
>
> The latest RHEL4 kernel for OpenVZ ((2.6.9-023stab016.2) available
> at http://openvz.org/download/kernel/rhel4/ *is vulnerable to the PRCTL
> exploit*: http://isc.sans.org/diary.php?storyid=1482
>
> example session of "nobody" running the exploit and getting a root shell:
>
> [root@mailin-02node tmp]# uname -a
> Linux mailin-02node.elitehosts.com 2.6.9-023stab016.2 #1 Thu Aug 10
> 23:39:42 MSD 2006 i686 i686 i386 GNU/Linux
> [root@mailin-02node tmp]# su nobody
> bash-3.00$ ls -ld 05
> -rwxr-xr-x 1 nobody nobody 13298 Oct 11 21:42 05
> bash-3.00$ ./05
>
> prctl() suidsafe exploit
>
> (C) Julien TINNES
>
> [+] Installed signal handler
> [+] We are suidsafe dumpable!
> [+] Malicious string forged
> [+] Segfaulting child
> [+] Waiting for exploit to succeed (~26 seconds)
> [+] getting root shell
> sh-3.00# whoami
> root
> sh-3.00# uname -a
> Linux mailin-02node.elitehosts.com 2.6.9-023stab016.2 #1 Thu Aug 10

> 23:41:42 MSD 2006 i686 i686 i386 GNU/Linux
> sh-3.00#
>
> --------------------------
> Avi Brender
> abrender@elitehosts.com <mailto:abrender@elitehosts.com>
> Elite Hosts, Inc
> --
> WARNING !!! This email message is for the sole use of the intended
> recipient(s) and may contain confidential and privileged information.
> Any unauthorized review; use, disclosure or distribution is prohibited,
> and could result in criminal prosecution. If you are not the intended
> recipient, please contact the sender by reply email and destroy all
> copies of the original message. This message is private and is
> considered a confidential exchange - public disclosure of this
> electronic message or its contents are prohibited.
> ----------------------
>
>
>
> -- ------------
>