Subject: sock_sendpage() kernel vulnerability
Posted by lukaschemp on Tue, 01 Sep 2009 07:21:52 GMT
View Forum Message <> Reply to Message

Hello,

Anybody have tested exploit for Linux kernel 2.4/2.6 sock_sendpage() on OpenVZ kernel in CentOS 5.X, it's vulnerable?

RHEL/CentOS has updated kernel to 2.6.18-128.7.1.el5 with no vulnerable.

Exploit: http://milw0rm.com/exploits/9545

Subject: Re: sock_sendpage() kernel vulnerability
Posted by Valmont on Tue, 01 Sep 2009 19:08:45 GMT
View Forum Message <> Reply to Message

Well, according opennet.ru we have also this sploit:

http://www.risesecurity.org/entry/illustrating-linux-sock_se ndpage-null-pointer/

and this:

http://grsecurity.net/~spender/wunderbar_emporium.tgz

Due lack of phys. access to my servers I can't check it now, but
changelog http://wiki.openvz.org/Download/kernel/rhel5/028stab064.4
don't have any notes about fixing CVE-2009-2692

Make it for hotfix:

Red Hat Enterprise Linux 4 and 5

Add the following entries to the end of the /etc/modprobe.conf file:

```
install pppox /bin/true
install bluetooth /bin/true
install sctp /bin/true
```

The sctp module cannot be unloaded from a running kernel if the module is already loaded; therefore, the above changes for /etc/modprobe.conf on Red Hat Enterprise Linux 4 and 5 require a reboot to take effect.

Subject: Re: sock_sendpage() kernel vulnerability
Posted by Valmont on Tue, 01 Sep 2009 19:11:27 GMT
View Forum Message <> Reply to Message

first link sploit is same as milworm.

Subject: Re: sock_sendpage() kernel vulnerability
Posted by Valmont on Tue, 01 Sep 2009 19:28:07 GMT
View Forum Message <> Reply to Message

Another point. According buzilla and changelog 2.6.18-128.7.1 fix also other bad thing (CVE-2009-2698). So this update imho is urgent.

Subject: Re: sock_sendpage() kernel vulnerability
Posted by lukaschemp on Tue, 01 Sep 2009 19:31:54 GMT
View Forum Message <> Reply to Message

But 2.6.18-128.7.1 from RHEL/CentOS repo is supported to use OpenVZ?

Subject: Re: sock_sendpage() kernel vulnerability
Posted by Valmont on Tue, 01 Sep 2009 19:45:27 GMT
View Forum Message <> Reply to Message

No, certainly no.

As another solution except waiting new openvz release - get from redhat/centos src.rpm necessary patches and recompile openvz kernel with them.