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.