Subject: Re: Linux kernel null pointer bug
Posted by lazy on Wed, 26 Aug 2009 07:17:25 GMT
View Forum Message <> Reply to Message

finist wrote on Wed, 26 August 2009 02:54Quote:but still it's possible to destabilize the kernel with a failed exploit attempt

Not exactly: you need to modify exploit to do this. But yes, it's possible, but again - from Hardware Node only.

Quote:and there is another bug fixed in RHSA-2009:1222-02
https://rhn.redhat.com/errata/RHSA-2009-1222.html
...
testing went threw ok, i will se if there will be any problems in production

Yes, we've already seen that, thank you.

I recall when when I started one of the exploits from 32 bit guest(64 bit host), its process got blocked in kernel space and I couldn't enter any other vps, reboot machine properly etc.
when I have some time I will recheck it (maybe after all I wasn't running 64.4 on that machine) exploit was modified to run without kernel symbols in /proc

patched machines are working fine, is applying mentioned patch is sufficient ? (debian is using this patch for etch kernel so i guess it's safe to think so)

thanks for Your answer
--
Lazy