Subject: Re: Linux kernel null pointer bug
Posted by lazy on Tue, 25 Aug 2009 19:20:02 GMT
View Forum Message <> Reply to Message

finist wrote on Tue, 18 August 2009 08:35Hi.

2.6.18-128.2.1.el5.028stab064.4 kernel (latest stable OVZ) is immune to the exploits on the issue.

The kernel is immune due to the fact that 64.4 kernel has the bypassing "mmap_min_addr" issue fixed:
http://blog.cr0.org/2009/06/bypassing-linux-null-pointer.htm l - description of the problem

Exploits for the current issue, in their turn, need this hole to gain root access.

but still it's possible to destabilize the kernel with a failed exploit attempt

and there is another bug fixed in RHSA-2009:1222-02
https://rhn.redhat.com/errata/RHSA-2009-1222.html
bug
https://bugzilla.redhat.com/show_bug.cgi?id=518034

tonight i'm rolling 64.4 with patches from upstream
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6
.git;a=commitdiff;h=1e0c14f49d6b393179f423abbac47f85618d3d46

testing went threw ok, i will se if there will be any problems in production