

## Re: rooted ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-09/0024.html>

---

**From:** Coleman (*cokane\_at\_cokane.org*)

**Date:** 09/10/04

To: Jason Rusch <kerberos\_daemon@infosec-rusch.com>

Date: Fri, 10 Sep 2004 13:40:45 -0400

I have found that chkrootkit can cause some false positives with this check alot. Basically this check takes the output of ps (or whatever means it uses to determine running procs) and compares that with what it sees in /proc/. If it finds any discrepencies, it dumps that info to you, and I suppose the claim that there may be an LKM rootkit installed is because that is a common way to hide processes, installing an LKM to modify the kernel structs. I have a high-traffic mailserver which constantly has quickly dying/starting procs for mail delivery (qmail), it causes this error much of the time.

On Thu, 2004-09-09 at 08:21, Jason Rusch wrote:

> *Sorry if this is not the correct forum,*

>

> *Curious a day or so after a up2date on a fedora 2 system, I noticed very sluggish behavior. After checking obvious things such as netstat, du, nmaping it from another machine and checking ps commands thoroughly I found nothing abnormal. I then moved onto running a few rootkit scanners, all showed cleaned (for what its worth of course), I used both the tarball and rpm chkrootkit and scanned my machine with both.*

>

> *The strange part is, is that the one ran from source showed everything to be ok, the rpm showed 23-35 hidden processes, possible LKM rootkit installed. now after running the cmd "  
/usr/lib/chkrootkit-0.43/chkproc -v" I found the processes within the /proc and checked the status/info on all. they were all sleeping process from application I run all the time (evolution, mozilla, nautilus ). I booted the machine in init3 and without X and I didnt have this problem.*

>

> *The machine normally boots in init5, now if I start X then the problem arises, now I dont know if this is the right forum, but I would not think that I am rooted (optimistically said) and this is some weird iissue from an update. I more note all the hidden processes were owned and ran under my user account. Any input from anyone would be great. and no I didnt get Tripwire installed or record a MD5sum record ooopps*

>

> *anyway just a day or so ago I read somewhere there may be a latency time diff. between the threads that are running and the chrootkit detection thus causing the discrepancy?*