

[SLE] chkroot claims top infected

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2004-01/4558.html>

From: David Herman (*mesamoo115_at_comcast.net*)

Date: 01/31/04

To: suse-linux-e@suse.com

Date: Sat, 31 Jan 2004 10:31:20 -0800

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

SuSE 9.0

Just ran chkroot (chkrootkit-0.43, Sat Dec 27 2003) and it gave the results

Checking `top'... INFECTED

and

Checking `lkm'... You have 5 process hidden for ps command

I found these commands were in an rpm updated w/ synaptic recently, ps_2003.11.17-18_i586.rpm. The file can be found at <ftp://ftp.gwdg.de/pub/linux/suse/apt/SuSE/9.0-i386/RPMS.suse-people>

I renamed top, re-installed the rpm but chkroot still shows the same result.

top's size is 81.5kb and has a modified date of 2004-01-20

#top -h

top: procps version 3.1.14

Is this an issue or is chkroot being fooled by the newer version?

I'm also curious about the "Checking `lkm'... You have 5 process hidden for ps command" result. Whats up with that?

Thanks for your ideas

dh

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.2 (GNU/Linux)

iD8DBQFAG/R+BwgxlylUsJARAixkAJ47XBzOML9Qzca7Nlfd2+sIcLbqKwCfWdwJ
ypIVdSAhtYrWMSHy37v/jfk=
=h9Le

-----END PGP SIGNATURE-----

SuSE: [SLE] chkroot claims top infected

--

Check the headers for your unsubscription address
For additional commands send e-mail to suse-linux-e-help@suse.com
Also check the archives at <http://lists.suse.com>
Please read the FAQs: suse-linux-e-faq@suse.com