

Re: [SLE] chkroot claims top infected

Source: <http://linux.derkeiler.com/Mailing-Lists/SuSE/2004-02/0109.html>

From: Thomas Jones (thomas.jones_at_linux-howtos.com)

Date: 02/02/04

To: suse-linux-e@suse.com

Date: Sun, 1 Feb 2004 22:07:59 -0800

On Sunday 01 February 2004 09:49 am, David Herman wrote:

> On Saturday 31 January 2004 11:14 pm, GarUlbricht7@netscape.net wrote:

>> *I am surprized that you have not posted this on*

>> *suse-security mailing list:*

>> http://www.suse.com/us/private/support/online_help/maillinglists/index.html

>>

>> *Or maybe you have and I just missed it.*

>

> -----snip-----

> *Actually I wasn't on that list until just now, I'll post there shortly*

> *unless someone beats me to it.*

>

> *I was really hoping that checkroot was giving a false positive. I did*

> *fill out the webform at feedback.suse but who knows how long that will*

> *take.*

>

> *see ya*

> --

> *dh*

> *Don't shop at GoogleGear.com!*

A couple notes:

Have you checked your system logs?

Did you have wither an tripwire or AIDE database prior?

Check for deleted(possibly trojaned) executables via:

```
# file /proc/[0-9]*/exe|grep '(deleted)'
```

Also extract the binary version from the installation CD of ps,ls,who ----- commonly trojaned executables onto a floppy from another system. Write protect it!

Then perform a compare of the valid(floppy) version against the possibly

SuSE: Re: [SLE] chkroot claims top infected

trojaned executable via:

```
# cmp /media/floppy/valid_exec /bin/trojan_exec
```

This will do a byte-by-byte comparison of both executables.

You can search for the debugging symbols from the "trojaned" executable via:

```
# nm trojan_exec | more
```

Also check for any ascii text in the executable via:

```
# strings -a trojan_exec | more
```

HTH.

thomas

--

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