

Re: World writable tarballs

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-04/msg06734.html>

- *From:* Mark Rosenstand <mark@xxxxxxxxxxxxx>
 - *Date:* Sun, 30 Apr 2006 19:08:15 +0200
-

On Sun, 2006-04-30 at 13:51 +0100, Alistair John Strachan wrote:

On Sunday 30 April 2006 13:36, Mark Rosenstand wrote:

On Sun, 2006-04-30 at 12:49 +0100, Alistair John Strachan wrote:

Going over old ground again, any administrator a) compiling the kernel as root or b) relying on GNU tar to make `_security policy decisions_` is completely insane.

Yes, GNU tar is acting insane. Given that GNU tar is the most widely used tar implementation (at least for extracting linux sources), why is the kernel packaged to exploit this insane behaviour?

I think you're missing the point. The tar archive can have whatever the hell permissions it likes; you as the user of tar and risking extraction as root should know what tar does and (if you care) take action to negate it.

Even back before the kernel tar files made every file writable by all, there were always a few files that were marked executable (!!) by all. Bottom line: you can't rely on the permissions in the tar files.

I think you are missing the point. The point is that the kernel source gets extracted with world writable permissions, without any reason.

I am fully aware that you cannot trust the permissions of extracted tar archives with GNU tar unless you explicitly add an unreasonably long argument, whereas other tar implementations require you to use the `p` flag.

The question is: Is it right to exploit this misbehaviour?

(You probably aren't aware of the recent bug found in the kernel build system

Re: World writable tarballs

where, if compilation was executed as root, it would overwrite the /dev/null node with a regular file -- now THAT'S a security problem!)

Yes, that is indeed a good argument for not building as root. But please try to stay on the fucking subject or be quiet.

—

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@xxxxxxxxxxxxxxxx

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>