

Re: World writable tarballs

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-04/msg06691.html>

- *From:* Alistair John Strachan <s0348365@xxxxxxxxxxxxx>
 - *Date:* Sun, 30 Apr 2006 12:49:16 +0100
-

On Sunday 30 April 2006 10:15, Heikki Orsila wrote:

On Sun, Apr 30, 2006 at 01:48:12AM +0100, Alistair John Strachan wrote:

There's no need to repeatedly discuss it.

I think there is. Sorry for wasting bandwidth.

It's a big security hole deliberately caused by the kernel people (files in the tar ball have og+w, so it's not problem in roots umask or tar). Real security needs `_simplicity_` but current file modes require unnecessary `_tricks_` for admins. There should be nothing against untarring files as root. In this case it makes sense too, because only the tar balls are crypto signed, not the individual files inside the tar ball, so root can conveniently just verify the crypto signature and untar the file without any race conditions or trusting other users. The only real alternative is to create an `_unnecessary_` trusted user to do tar ball handling.

PS. this file permission bug almost bit me. People make errors and this one is potentially a big privilege escalation, because it potentially turns normal application bugs into root privileges.

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.

The only "trick" here is tar's decision to not apply umask, or root uid/gid, to files in a tar when extracted as root. This might make sense for tars that you created and want to extract again (say restoring a backup), but it certainly NEVER makes sense for files downloaded off the Internet.

If people are insistent that they must extract and compile things as root, at the very least you should have the following in root's `~/.bashrc`:

```
alias tar='tar --no-same-permissions --no-same-owner '
```

Re: World writable tarballs

Then if you want the default (imo flawed) tar behaviour, you can just call tar directly.

Really, people that complain about security should have a modicum of a clue; allowing a tar file that _somebody else_ applied _their_ security policy, to define yours, is a deeply flawed concept. umask is there for a reason.

--

Cheers,
Alistair.

Third year Computer Science undergraduate.
1F2 55 South Clerk Street, Edinburgh, UK.

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@xxxxxxxxxxxxxxxxx
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>