

Re: World writable tarballs

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-04/msg06680.html>

- *From:* Heikki Orsila <shd@xxxxxxxxxx>
 - *Date:* Sun, 30 Apr 2006 09:15:01 +0000
-

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.

--

Heikki Orsila Barbie's law:

heikki.orsila@xxxxxx "Math is hard, let's go shopping!"

<http://www.iki.fi/shd>

-

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/>