

Re: Reflections on Trusting Trust

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-11/0092.html>

From: Kris Kennaway (kris_at_obsecurity.org)

Date: 11/30/05

Date: Wed, 30 Nov 2005 04:02:48 -0500
To: ?d?m Szilveszter <adamsz@mailpont.hu>

On Wed, Nov 30, 2005 at 09:55:24AM +0100, ?d?m Szilveszter wrote:

> *On Sze, November 30, 2005 12:43 am, Colin Percival mondta:*
> > *Even before you get to that point, you have to worry about making sure*
> > *that the build clients are secure. One possibility which worries me a*
> > *great deal is that a trojan in the build code for a low-profile port*
> > *(e.g., misc/my-port-which-nobody-else-uses) could allow an attacker to*
> > *gain control of a build client (and then insert trojans into packages*
> > *which are built there).*
>
> *Which practically begs the question: could we, pretty please, change the*
> *defaults and stop encouraging people from downloading distfiles and*
> *compiling them when using the ports tree as *root*? (shudder) There is*
> *exactly zero reason for this that I can think of apart from some "well*
> *it's more convenient that way" arguments.*

And of course that some ports don't build as non-root :-)

If you're willing to fix them (there may be a lot), I could schedule a full port build done as non-root so you can start work.

Kris

-
- application/pgp-signature attachment: [stored](#)