

RE: /dev/random on Linux

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-05/msg04161.html>

- *From:* "Zvi Gutterman" <zvi@xxxxxxxxxx>
 - *Date:* Tue, 16 May 2006 16:54:00 +0300
-

Hello All,

I did not get any answer from Matt and was sure that it was of no interest. This was my mistake, sorry for not sending it earlier to more people.

I will be very happy to discuss any aspect of the paper and we do suggest ways we think can improve the /dev/random security (a very simple issue for example is implementing quotas on the consumption of random numbers)

Thanks,

Zvi

-----Original Message-----

From: Muli Ben-Yehuda [<mailto:mulib@xxxxxxxxxx>]

Sent: Tuesday, May 16, 2006 11:29 AM

To: Kyle Moffett

Cc: Alan Cox; Jonathan Day; linux-kernel@xxxxxxxxxxxxxxxxxx; Zvika Gutterman

Subject: Re: /dev/random on Linux

On Tue, May 16, 2006 at 04:15:19AM -0400, Kyle Moffett wrote:

On May 15, 2006, at 22:50, Muli Ben-Yehuda wrote:

On Mon, May 15, 2006 at 11:41:07PM +0100, Alan Cox wrote:

A paper by people who can't work out how to mail
linux-kernel or
vendor-sec, or follow "REPORTING-BUGS" in the source,

Zvi did contact Matt Mackall, the current /dev/random maintainer, and was very keen on discussing the paper with him. I don't think he got any response.

So he's demanding that one person spend time responding to his

RE: /dev/random on Linux

paper?

Who said anything about demanding? he wanted to discuss the paper. He received no response (AFAIK). Please don't read more into it.

The "maintainer" for any given piece of the kernel is the entry in MAINTAINERS *and* linux-kernel@xxxxxxxxxxxxxxxx *and* the appropriate sub-mailing-list.

For security related information, it is sometimes best not to tell the whole world about it immediately (although you should definitely tell the whole world about it eventually). It should've probably been posted to lkml when mpm didn't respond, I agree. I'll take the blame for not suggesting that to Zvi.

Cheers,
Muli

—

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/>

RE: /dev/random on Linux