

Re: security issues

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2006-03/msg01353.html>

- *From:* Colin Watson <cjwatson@xxxxxxxxxx>
 - *Date:* Tue, 14 Mar 2006 12:29:41 +0000
-

On Mon, Mar 13, 2006 at 06:04:20PM -0600, Lamp wrote:

Why on God's green earth was the password ever written to a file in the first place?!?!??

It was obviously never meant to be; multiple defences against it being written to disk failed simultaneously. Those of you who are assuming that this was because of the equivalent of "fprintf(log, password);" assume wrongly; we aren't quite *that* careless! It was significantly more complicated than that.

Here's my explanation of the problem that I posted to osnews.com and the Ubuntu forums:

=====

The Ubuntu installer (like Debian) uses a framework called debconf to do all its user interaction; that framework has a backend database which stores all the answers, which is where passwords ended up being stored for this vulnerability. Naturally, when you're asking for passwords using debconf, you take a lot of care to clean them out of the database afterwards: we explicitly clear them out in the password-asking code pretty much as soon as we can, and we have a separate database for the answers to password questions which isn't copied to the directory of installer log files in the final installed system. This had all been working well for some time (e.g. in Hoary).

Unfortunately, the way we arranged for the password question to be asked in the first stage of the Breezy installer meant that two debconf databases were involved rather than one, and the passwords only got cleared out of one of those databases. Even this would have been OK if it weren't for the fact that some changes we needed to make in cdebconf for other reasons in Breezy (I've yet to track down the exact changesets involved, but never mind) broke the mechanism that was supposed to make sure that passwords ended up in a separate database. Sigh.

As for why we didn't notice the problem in Breezy when this was fixed in

Re: security issues

Dapper, well, that's because the fix in Dapper was part of a massive installer reorganisation

(<http://riva.ucam.org/~cjwatson/blog/ubuntu/2006-01-03-single-stage-installer.html>)

and it was really just fixed by accident. So it goes.

Anyhow, I've fixed this just about as soon as was humanly possible for me, and take it extremely seriously. While perhaps for some of you it's too little too late, we'll do everything we can to install better defences against this kind of thing in future.

In briefer terms, the "installer log" in question was a dump of database contents; the password was never meant to be written to any database, and if it was written it was meant to be to a different database which would only exist in the installer ramdisk and which wouldn't end up on the installed system. Both these defences failed due to problems that, unfortunately, I'm pretty sure would have escaped code review; our chief problem was simply that nobody thought to grep the system for the password before release. That's a problem that's easy to criticise with hindsight ...

The attached diff fixes the core of the problem, although some other changes were necessary to fix a related problem with preseeded passwords. More defences are of course being implemented; the database dumps in question (although they are often necessary to debug installer problems) will be readable by root only from now on.

Cheers,

--

Colin Watson [cjwatson@xxxxxxxxxx]

--

ubuntu-users mailing list

ubuntu-users@xxxxxxxxxxxxxxxxxx

<https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>