

Re: Vote for new Ubuntu Feature----Let's try it again ---- and without getting all religious about it

Re: Vote for new Ubuntu Feature----Let's try it again ---- and without getting all religious about it

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2007-01/msg00975.html>

- *From:* "Jeffrey F. Bloss" <jbloss@xxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 11 Jan 2007 21:11:30 -0500
-

Derek Broughton wrote:

Don't be silly – applications
do do this, and as
Chanchao
says it isn't Unix blasphemy.

Yes, and if you read back through the thread
I thought I'd made
this clear when I stated quite plainly that
there's two avenues
of attack to this "problem"... either neutering
the Linux/Unix
security model, or convincing every Tom,
Dick, And Harry software
author to rewrite their wares in a compliant
and *secure* way.
Like I said, it's not gonna happen in our
lifetime or likely any
other.

But right here, Chanchao just asked for it to be done on a
per-application basis, and you told him that he was
castrating the
unix security model. His suggestion most certainly does not.

It absolutely does! Software authors changing permissions
mid-stream is a dire security problem. And other applications do
NOT do this. The Linux kernel won't permit it except in the most
unusual of circumstances, if at all. If you examine the few
examples where people are being tricked into thinking it happens
you'll find that they're all all exec-ing new processes with admin
privilege. "Update Manager" execs a command shell for instance.

Re: Vote for new Ubuntu Feature----Let's try it again ---- and without getting all religious about it

Exactly! Which is all that chanchao suggested. There is no privilege escalation or security castration happening.

I'm sorry, but third party software authors writing code that spawns privilege escalation after the fact is a security problem any way you slice it. Shell or no shell, sudo or otherwise, you sitting there with a potentially harmful buffer of Joe User modified data and trusting that said authors have properly implemented an interface to whatever privilege escalation mechanism they decided to use, just before it's plastered across your hard drive.

No thanks. Like I said it's so trivially easy to avoid being in this position in the first place even a perfect implementation isn't worth the risk. Personally, I don't even think UM should do it. Of course I don't make those decisions, and I can see how it's almost necessary given the fact that its intended function is notifying users of administrative updates. The alternative of course is to log in as root to get your notifications. The trade off is obvious. It's not when inattentive users simply neglect to consider the fact that they're trying to edit a file in /etc/not/your/stuff.

This is a completely different thing than Gedit elevating it's own permissions so it can save a file.

And neither of us suggested it should – his suggestion was that gedit should run sudo to cp a temp file, and if that wasn't clear enough I _specifically_ said that.

You can do that yourself with a script. Or manually. There's no need for any software authors to be involved,

Of course you can, and of course there's not – which is why your reaction is completely out of line with the reality of the situation.

Nobody has yet explained to me what the problem is with simply using your brain for something besides keeping your skull from caving in,

Hey, I've got no problem with the system as-is, but you just went off the deep end with a reasonable (if unworkable) suggestion from Chanchao.

Re: Vote for new Ubuntu Feature----Let's try it again ---- and without getting all religious about it 2

Re: Vote for new Ubuntu Feature----Let's try it again ---- and without getting all religious about it

here's a free clue that might help stave off the ruination of Linux. ;) If it doesn't reside in your \$HOME you probably don't have permission to change it...

Except that that's less and less true. Probably 90% of the people reading this list have full sudo rights on their machine. They may have 2 or 3 other people using the machine who don't have those rights, but the folks reading this list are the godlike ones :-)
Again, a better way of putting it is probably that if it doesn't exist in your \$HOME, you want to think twice about changing it.

--

? Outside of a dog, a book is a man's best friend.

(o o) Inside of a dog, it's too dark to read.

-oOO-(_)-OOo-----[Groucho Marx]--

grok! Registered Linux user #402208

Attachment: signature.asc

Description: PGP signature

--

ubuntu-users mailing list

ubuntu-users@xxxxxxxxxxxxxxxxxx

Modify settings or unsubscribe at: <https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>