

## Re: gzip TOCTOU file-permissions vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-04/0221.html>

---

**From:** Derek Martin ([code\\_at\\_pizzashack.org](mailto:code_at_pizzashack.org))

**Date:** 04/14/05

Date: Thu, 14 Apr 2005 12:11:06 -0400

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)

On Thu, Apr 14, 2005 at 09:27:11AM -0600, Mark Senior wrote:

> > *From: Derek Martin [mailto:code@pizzashack.org]*

> > *Sent: April 13, 2005 08:50*

If you can, I might suggest configuring your e-mail client not to attribute e-mail addresses in replies (at least to mailing lists)...

It doesn't solve the problem by any means, but it reduces the availability of e-mail addresses in web archives which can be harvested. Mailing lists can easily be configured to obscure addresses in their web archives, but often this doesn't extend to addresses posted in the body of the e-mail itself... :)

> > *The open() call is at fault here. If instead of being called with a mode of RW\_USER, it is called with the final intended access mode, there is no need to later call chmod(), and the problem is averted.*

>

> *One wrinkle – if the file is not intended to have user write permission on it, and gzip (unzip/cpio/pax...) initially created it with the intended permissions, there would be no way to then write the file.*

Excellent point, which I overlooked. So the patch which I posted (whether it shows up on bugtraq is an entirely different question...) is worthless. Sigh. ;- ) I momentarily confused root's ability to write to any file regardless of access permissions with a fictitious user ability to write to their own files, regardless of write access. Too bad... that ability would make for a nice solution to the problem! [sheepish grin]

> *The problem, to my understanding, is that the program opens the file by name, then closes it, and then chmod's it, again referring to it by name. During which time, as you pointed out, we could be dealing with a different inode.*

Yeah, that's the problem.

SecurityFocus Bugtraq: Re: gzip TOCTOU file-permissions vulnerability

- > *If the program kept the file open, and used fchmod to change its*
- > *permissions, referring to it by file descriptor, you could be more sure*
- > *that it was the same inode it had just been writing to.*

That would do the trick. The question becomes one of how portable fchmod() is... My programming experience is unfortunately limited to platforms which are pretty POSIX compliant, so I can't even guess...

--

Derek D. Martin

<http://www.pizzashack.org/>

GPG Key ID: 0x81CFE75D

- 
- application/pgp-signature attachment: stored