

Re: [patch] rm can have undesired side-effects

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2006-10/msg00236.html>

- *From:* Peter Jeremy <peterjeremy@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 30 Oct 2006 19:38:49 +1100
-

On Sun, 2006-Oct-29 18:11:54 -0800, perryh@xxxxxxxxxxxxxxxx wrote:

I think a very strong case can be made that the **intent** of `-P` -- to prevent retrieval of the contents by reading the filesystem's free space -- implies that it should affect only the "real" removal of the file, when its blocks are released because the link count has become zero.

...

In this interpretation, "rm -P" when the link count exceeds 1 is an erroneous command.

I agree. Doing "rm -P" on a file with multiple links suggests that the user is unaware that there are multiple links. I don't think that just unlinking the file and issuing a warning is a good solution because it's then virtually impossible to locate the other copy(s) of the file, which remains viewable. I believe this is a security hole.

Consider: In FreeBSD, it is possible to create a hardlink to a file if you are not the owner, even if you can't read it. Mallory may decide to create hardlinks to Alice's files, even if he can't read them today on the off-chance that he may be able to circumvent the protections at a later date. Unless Alice notices that her file has a second link before she deletes it, when she issues "rm -P", she will lose her link to the file (and her only way of uniquely identifying it) whilst leaving the remaining link to the file in Mallory's control.

--

Peter Jeremy

Attachment: [pgpYQi4f8nIkI.pgp](#)

Description: PGP signature