

## Re: Call for review: restricted hardlinks.

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-03/0083.html>

---

**From:** Pawel Jakub Dawidek (*pjd\_at\_FreeBSD.org*)

**Date:** 03/08/04

Date: Mon, 8 Mar 2004 23:08:28 +0100

To: "Georg-W. Koltermann" <gwk@rahn-koltermann.de>

On Mon, Mar 08, 2004 at 10:10:38PM +0100, Georg-W. Koltermann wrote:

+> When you restrict links, do you want to restrict copying as well?

+>

+> Seems somewhat paranoid to me. You already need write permission on the

+> directory where you create the link, and permissions are checked against

+> the inode on open(2) anyway.

This is because this gives an attacker some possibilities.

For example he is able to create hard link to some set-uid binary.

After some time, a security-related bug will be found in this application,

administrator will change it with good version, but old, vulnerable

version will be still in system.

Administrator have to be really careful when fixing such problems

and check number of hard links or just remove such program using 'rm -P'.

--

Pawel Jakub Dawidek

pjd@FreeBSD.org

FreeBSD committer

<http://www.FreeBSD.org>

<http://garage.freebsd.pl>

Am I Evil? Yes, I Am!

- 
- application/pgp-signature attachment: [stored](#)