

Re: Call for review: restricted hardlinks.

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-03/0088.html>

From: Robert Watson (rwatson_at_FreeBSD.org)

Date: 03/10/04

Date: Tue, 9 Mar 2004 19:33:16 -0500 (EST)
To: "Georg-W. Koltermann" <gwk@rahn-koltermann.de>

On Mon, 8 Mar 2004, 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.*

The "classic hard link attack" is to find a writable directory in a partition containing setuid/setgid binaries, hard link them all to that directory, then wait for an exploit to be discovered in one of them. The administrator will apply the patches, rebuild, binary update, or whatever, and think they're covered, but the attacker still has a reference that can be executed later. This might be employed against `/usr/{bin,sbin,local}` using `/usr/tmp`, or `{/sbin,/bin}` using `/tmp` in default file system layouts.

Robert N M Watson FreeBSD Core Team, TrustedBSD Projects
robert@fledge.watson.org Senior Research Scientist, McAfee Research

- >
- > *My \$0.0002.*
- >
- > --
- > *Regards,*
- > *Georg.*
- >
- > *Am Mo, den 08.03.2004 schrieb Pawel Jakub Dawidek um 10:36:*
- > > *Hi.*
- > >
- > > *I've no response from so@ in this topic, probably because leak of time,*
- > > *so I'll try here.*
- > >
- > > *Here is a patch that I'm planing to commit:*
- > >
- > > http://people.freebsd.org/~pjd/patches/restricted_hardlinks.patch
- > >

FreeBSD-Security: Re: Call for review: restricted hardlinks.

> > *It adds two new sysctls:*
> >
> > *security.bsd.hardlink_check_uid*
> > *security.bsd.hardlink_check_gid*
> >
> > *If sysctl security.bsd.hardlink_check_uid is set to 1, unprivileged users*
> > *are not permitted to create hard links to files not owned by them.*
> > *If sysctl security.bsd.hardlink_check_gid is set to 1, unprivileged users*
> > *are not permitted to create hard links to files if they are not member*
> > *of file's group.*
> >
> > *For now user is able to create hardlinks to any files.*
>
>
> _____
> *freebsd-security@freebsd.org mailing list*
> <http://lists.freebsd.org/mailman/listinfo/freebsd-security>
> *To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"*
>

freebsd-security@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-security>
To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"