

Re: HEADS UP: Re: FreeBSD Security Advisory FreeBSD-SA-07:01.jail

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-01/msg00029.html>

- *From:* Dirk Engling <erdgeist@xxxxxxxxxxxxx>
 - *Date:* Tue, 16 Jan 2007 03:17:10 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Colin Percival wrote:

No. `cp -f` unlinks the existing file and creates a new file, but will still follow a symlink if one is created between the "unlink" syscall and the "open" syscall.

```
/* remove existing destination file name,  
 * create a new file */  
(void)unlink(to.p_path);  
if (!lflag)  
to_fd = open(to.p_path, O_WRONLY | O_TRUNC | O_CREAT,  
fs->st_mode & ~(S_ISUID | S_ISGID));
```

You are right. Atomically in binary is not atomical enough.

`mv` in its `rename()`-form will do the job, so we need to create a file in `.` by `mktemp` and `mv` it to the real name when filled.

Regards

erdgeist

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.3 (Darwin)

iD8DBQFFrDWmImmQdUyYEgkRAgSgAJ0c5mcaM4LByBUE0LC1Iqdj8ZFSAACdF9qM
fFETX4I+Fvue0u+343bBG8c=

=MkSh

-----END PGP SIGNATURE-----

freebsd-security@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxxxx"