

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

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-01/msg00009.html>

- *From:* Colin Percival <cperciva@xxxxxxxxxxxx>
 - *Date:* Thu, 11 Jan 2007 20:29:25 -0800
-

Philipp Wuensche wrote:

Colin Percival wrote:

In the end we opted to reduce functionality (the jail startup process is no longer logged to /var/log/console.log inside the jail)

Thats a bummer, when Dirk showed me this problem the first time my ideas for fixing this problem without losing the functionality where changing flags on the file so it can't be removed or/and checking if it is really a file or a symlink instead. Of course you have to check if /var/log has symlinked parent directories before.

First is quite problematic and setting flags on file is something scripts which create a jail in the first place probably have to bother with so option two would be my approach. Did I miss a possible problem with that idea?

Assuming that "option two" means "use file flags to make sure that the host can write to the jailed /var/log/console.log securely", setting the sunlnk flag on the jail's /var and /var/log would probably break many jails -- for one thing, log rotation would become impossible. Then there's the problem of systems with chflags_allowed=1...

(filesystems which are mounted via per-jail
fstab files should not be mounted on symlinks -- if you do this, adjust your
fstab files to give the real, non-symlinked, path to the mount point), and

If I understand the patch correct it checks recursive all parent directories of a mountpoint in `is_symlinked_mountpoint()`, wouldn't it be better to just check for a symlinked parent directory up to and not including `${_rootdir}`?

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

This option never occurred to me; I think it would work, but it would require canonicalizing the jail root path... even if I had thought of this, I might have decided to avoid this on the basis that complexity == bugs == bad for security patches.

Colin Percival

freebsd-security@xxxxxxxxxxx mailing list

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

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