

Re: security.bsd.see_other_uids for jails

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2006-05/msg00331.html>

- *From:* Robert Watson <rwatson@xxxxxxxxxxx>
 - *Date:* Mon, 29 May 2006 18:47:32 +0100 (BST)
-

On Mon, 29 May 2006, Anatoli Klassen wrote:

David Malone wrote:

On Sun, May 28, 2006 at 03:46:06PM +0200, Anatoli Klassen wrote:

if security.bsd.see_other_uids is set to 0, users from the main system can still see processes from jails if they have (by accident) the save uid.

For me it's wrong behavior because the main system and the jail are two different systems where uids are independent.

You could try the following (untested) patch to the MAC seeotheruid module. You'd need to compile a kernel with the MAC option and then:

Thanks for the patch, maybe I'll need something like that for my environment.

But my question is if it's really intended that jail is not real virtual system but just a way to limit interaction from jail to host and not vice versa.

If it's the case than this has to be specified in jail(8).

Yes, this is a documentation bug. It is more precise to think of jail as a subsetting service than a virtualizing service: processes in jails see a subset of the system resources, rather than virtualized versions. So, for example, they see a subset of the file system name space, a subset of the IP/port name space, a subset of the process list, etc. This means that applications in the "host" environment overlap with the jail environments by virtue of also having access to that subset, as they can directly name files in the file system subset, IP and port bindings, processes, and so on. This does appear unclear from a quick skim of the man page, so something on the order of the above, with practical suggestions on what this implies, is required in the page.

Robert N M Watson

freebsd-hackers@xxxxxxxxxxx mailing list

Re: security.bsd.see_other_uids for jails

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

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