

Re: Sandboxing

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2006-11/msg00009.html>

- *From:* Lowell Gilbert <frebsd-security-local@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 08 Nov 2006 09:08:02 -0500
-

"mal content" <artifact.one@xxxxxxxxxxxxxxxx> writes:

On 08/11/06, mal content <artifact.one@xxxxxxxxxxxxxxxx> wrote:

Hi.

This is mostly hypothetical, just because I want to see how knowledgeable people would go about achieving it:

I want to sandbox Mozilla Firefox. For the sake of example, I'm running it under my own user account. The idea is that it should be allowed to connect to the X server, it should be allowed to write to ~/.mozilla and /tmp.

I expect some configurations would want access to audio devices in /dev, but for simplicity, that's ignored here.

All other filesystem access is denied.

Ready...

Go!

MC

I forgot to add: Use of TrustedBSD extensions is, of course, allowed.

Putting an X Windows application in a sandbox is kind of silly. After all, X has to have direct access to memory. A virtual machine approach, with a whole virtual set of memory, might make more sense. I use that (via qemu), although not for exactly the same reasons.

frebsd-security@xxxxxxxxxxxxx mailing list

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

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