

Re: bktr(4) risk?

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2006-10/msg00052.html>

- *From:* John-Mark Gurney <gurney_j@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 9 Oct 2006 16:26:50 -0700
-

Jonathan Chen wrote this message on Mon, Oct 09, 2006 at 17:37 -0400:

While trying to resurrect meteor(4), I've been looking over the bktr driver. It seems that the bktr driver implements the METEORSVIDEO ioctl, which appears to allow userland programs to specify a physical memory address to which the bktr hardware should dump it's output. At first

Yes, it does...

glance, this seems like a rather bad idea, as this would allow anyone armed with the bktr file descriptor to arbitrarily trash any memory, and the bktr device comes with a friendly default permission of 0444.

The only reason I can think of to use this ioctl would be if you wanted the image you're capturing to be directly dumped into video memory. This

This is very common... It allows the bktr driver to dump the frames directly to the memory of your video card... This makes watching live tv watchable...

doesn't seem too useful a task for a video capture card to be doing. Perhaps we should put a test for write access in there or just eliminate the ioctl altogether. It should be noted that the meteor driver had this ioctl ifdef'ed out prior to its removal.

Hmmm... I think I'll go ahead and put in a compatibility ioctl based on the way I did the zoran driver, and schedule the removal of the ioctl..

Disclaimer: I don't have access to a bktr myself, nor am I very familiar with the intricacies of DMA, so someone with the expertise or the hardware should check my reasoning or test an exploit before panicing.

Re: bktr(4) risk?

John-Mark Gurney Voice: +1 415 225 5579

"All that I will do, has been done, All that I have, has not."

freebsd-hackers@xxxxxxxxxxx mailing list

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

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