

## Re: ide-cd problems

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2004-07/6454.html>

---

**From:** Zinx Verituse ([zinx\\_at\\_epicsol.org](mailto:zinx_at_epicsol.org))

**Date:** 07/31/04

Date: Sat, 31 Jul 2004 16:02:57 -0500

To: Jens Axboe <[axboe@suse.de](mailto:axboe@suse.de)>

On Sat, Jul 31, 2004 at 10:00:36PM +0200, Jens Axboe wrote:

> *On Sat, Jul 31 2004, Zinx Verituse wrote:*

>> *On Sat, Jul 31, 2004 at 05:36:10PM +0200, Jens Axboe wrote:*

>>> *On Fri, Jul 30 2004, Zinx Verituse wrote:*

>>>> *I'm going to bump this topic a bit, since it's been a while..*

>>>> *There are still some issues with ide-cd's SG\_IO, listed from*

>>>> *most important as perceived by me to least:*

>>>>>

>>>>> *\* Read-only access grants you the ability to write/blank media in the drive*

>>>>> *\*(with above) You can open the device only in read-only mode.*

>>>>

>>> *That's by design. Search linux-scsi or this list for why that is so.*

>>

>> *The only thing I can find on the linux-scsi list is referring to sg*

>> *devices, which are on a different device node from the non-generic*

>> *device. This means you can still allow users read access to the disk*

>> *without allowing them to send random commands to the disk -- this isn't*

>> *currently possible with the IDE interface, since the device with*

>> *generic access is the same as the one with the original read/cdrom*

>> *commands access.*

>>

>> *As it is, it's impossible grant users read-only access to an IDE cd-rom*

>> *without allowing them to do things like replacing the firmware with a*

>> *malicious/non-working one.*

>>

>> *Generic access allowing such things is fine; but only if we can grant*

>> *non-generic access without granting generic access.*

>

> *If you want it to work that way, you have to have a pass-through filter*

> *in the kernel knowing what commands are out there (including vendor*

> *specific ones). That's just too ugly and not really doable or*

> *maintainable, sorry.*

>

> *If you have access to issue ioctls to the device, you have access to*

> *send it arbitrary commands - period.*

I don't believe command filtering is necessary, since all of the

## Linux-Kernel: Re: ide-cd problems

ide-cd ioctls are still there (ioctls that allow playing, reading, etc)  
Only the SG\_IO ioctl itself would have to be checked (i.e., not each individual command available with SG\_IO, just the overall ioctl itself, categorizing all of SG\_IO more or less as raw IO. If this isn't doable with the current design, then the ide-cd interface should at least be very conspicuously documented as being extremely insecure as far as "read" access is concerned, as I know I wouldn't expect users to be able to overwrite my drive's firmware simply by granting the read access.

--

Zinx Verituse

<http://zinx.xmms.org/>

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to [majordomo@vger.kernel.org](mailto:majordomo@vger.kernel.org)

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>