

Re: [stable] [PATCH 1/2] sd: fix memory corruption by sd\_read\_cache\_type

## Re: [stable] [PATCH 1/2] sd: fix memory corruption by sd\_read\_cache\_type

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-02/msg09196.html>

---

- *From:* Al Viro <[viro@xxxxxxxxxxxxxxxxxxx](mailto:viro@xxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 26 Feb 2006 14:57:51 +0000
- 

On Sun, Feb 26, 2006 at 08:34:10AM -0600, James Bottomley wrote:

Well, OK, I agree allowing us to request data longer than the actual buffer is a problem. However, I don't exactly see how this actually causes corruption, since even the initio bridge only sends 12 bytes of data, so we should stop with a data underrun at that point (however big the buffer is)

scsi\_mode\_sense() does memset(buffer, 0, len). You don't need corrupting data to come from device - 10Kb of zeroes into 512-byte kmalloc'ed buffer will do the job just fine...

ACKed in that form.

-

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

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

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