Subject: [patch i2o 2/6] wrong memory access in i2o_block_device_lock()
Posted by vaverin on Tue, 15 May 2007 12:43:17 GMT
View Forum Message <> Reply to Message

This patch fixes access to memory that has not been allocated:
i2o_msg_get_wait() can returns errors different from I2O_QUEUE_EMPTY. But the result is checked only against this code. If it is not I2O_QUEUE_EMPTY then we dereference the error code as the pointer later.

Signed-off-by: Vasily Averin <vvs@sw.ru>

```
--- lk2.6/drivers/message/i2o/i2o_block.c
+++ lk2.6/drivers/message/i2o/i2o_block.c
@@ -215,7 +215,7 @@ static int i2o_block_device_lock(struct
  struct i2o_message *msg;

  msg = i2o_msg_get_wait(dev->iop, I2O_TIMEOUT_MESSAGE_GET);
- if (IS_ERR(msg) == I2O_QUEUE_EMPTY)
+ if (IS_ERR(msg))
   return PTR_ERR(msg);

  msg->u.head[0] = cpu_to_le32(FIVE_WORD_MSG_SIZE | SGL_OFFSET_0);
```