

## Re: Zeroed pages returned for heap

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-06/1807.html>

---

**From:** Nagendra Singh Tomar (*nagendra\_tomar\_at\_adaptec.com*)

**Date:** 06/08/05

Date: Wed, 8 Jun 2005 09:38:05 +0530 (IST)

To: Peter Staubach <staubach@redhat.com>

On Tue, 7 Jun 2005, Peter Staubach wrote:

> *Nagendra Singh Tomar wrote:*

>

> > *Hi all,*

> > *The short version first.*

> > *Is it OK for an application (a C library implementing malloc/calloc is*

> > *also an application) to assume that the pages returned by the OS for heap*

> > *allocation (either directly thru brk() or thru mmap(MAP\_ANONYMOUS)) will*

> > *be zero filled.*

> >

>

> *An application which makes assumptions about the contents of newly allocated*

> *memory would seem to be making very dangerous assumptions.*

That's what glibc does. Ulrich confirmed that. I would say that's not a bad optimization on glibc's part as it does not really make sense to zero out a memory again in user space if we know for sure that new heap memory that kernel hands over to us will be zeroed. I'm not sure though whether this is a documented kernel ABI.

>

> *Ignoring that, would it not be considered to be a security violation to hand*

> *pieces of memory to applications without erasing the old contents of the*

> *pages?*

I understand that for a desktop/server running Linux but not for an embedded box where all the applications that run on the box is controlled by you.

Thanx,

Tomar

— You have moved the mouse. Windows must be restarted for the changes to take effect.

—

Linux-Kernel: Re: Zeroed pages returned for heap

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/>