

Re: user malloc from kernel

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2003-09/0474.html>

From: Peter Pentchev (*roam_at_ringlet.net*)

Date: 09/29/03

Date: Mon, 29 Sep 2003 18:56:13 +0300

To: Pawel Jakub Dawidek <nick@garage.freebsd.pl>

On Mon, Sep 29, 2003 at 05:47:41PM +0200, Pawel Jakub Dawidek wrote:

> *On Mon, Sep 29, 2003 at 05:22:47PM +0300, earthman wrote:*

> > *how to allocate some memory chunk*

> > *in user space memory from kernel code?*

> > *how to do it correctly?*

>

> *Here you got sample kernel module which do this:*

>

> <http://garage.freebsd.pl/usmalloc.tgz>

> <http://garage.freebsd.pl/usmalloc.README>

Errrr... but won't this interfere **badly** with userland programs which attempt to allocate memory after making the syscall in question? I mean, won't the application's memory manager attempt to allocate the next chunk of memory right over the region that you have stolen with this brk(2) invocation? Thus, when the application tries to write into its newly-allocated memory, it will overwrite the data that the kernel has placed there, and any attempt to access the kernel's data later will fail in wonderfully unpredictable ways :)

G'luck,

Peter

--

Peter Pentchev roam@ringlet.net roam@sbnd.net roam@FreeBSD.org

PGP key: <http://people.FreeBSD.org/~roam/roam.key.asc>

Key fingerprint FDBA FD79 C26F 3C51 C95E DF9E ED18 B68D 1619 4553

No language can express every thought unambiguously, least of all this one.

- application/pgp-signature attachment: [stored](#)