Subject: Re: [PATCH v2 01/29] slab: dup name string
Posted by David Rientjes on Tue, 15 May 2012 22:04:14 GMT
View Forum Message <> Reply to Message

On Fri, 11 May 2012, Glauber Costa wrote:

> diff --git a/mm/slab.c b/mm/slab.c
> index e901a36..91b9c13 100644
> --- a/mm/slab.c
> +++ b/mm/slab.c
> @@ -2118,6 +2118,7 @@ static void __kmem_cache_destroy(struct kmem_cache *cachep)
> kfree(l3);
> }
> }
> + kfree(cachep->name);
> kmem_cache_free(&cache_cache, cachep);
> }
>
> @@ -2526,7 +2527,7 @@ kmem_cache_create (const char *name, size_t size, size_t align,
> BUG_ON(ZERO_OR_NULL_PTR(cachep->slabp_cache));
> }
> cachep->ctor = ctor;
> - cachep->name = name;
> + cachep->name = kstrdup(name, GFP_KERNEL);
>
> if (setup_cpu_cache(cachep, gfp)) {
> __kmem_cache_destroy(cachep);

Couple problems:

 - allocating memory for a string of an unknown, unchecked size, and

 - could potentially return NULL which I suspect will cause problems
   later.