Subject: [PATCH] IPC: access to unmapped vmalloc area in grow_ary()
Posted by Kirill Korotaev on Mon, 17 Apr 2006 11:32:04 GMT
View Forum Message <> Reply to Message

grow_ary() should not copy struct ipc_id_ary (it copies new->p, not
new). Due to this, memcpy() src pointer could hit unmapped vmalloc page
when near page boundary.

Found during OpenVZ stress testing

Signed-Off-By: Alexey Kuznetsov <kuznet@ms2.inr.ac.ru>
Signed-Off-By: Kirill Korotaev <dev@openvz.org>

```
diff -urp ../git/linux-2.6.16-workgpl/ipc/util.c linux-2.6.16/ipc/util.c
--- ../git/linux-2.6.16-workgpl/ipc/util.c 2006-04-13 16:01:47.000000000 +0400
+++ linux-2.6.16/ipc/util.c 2006-04-13 16:01:05.000000000 +0400
@@ -187,8 +187,7 @@ static int grow_ary(struct ipc_ids* ids,
  if(new == NULL)
   return size;
  new->size = newsize;
- memcpy(new->p, ids->entries->p, sizeof(struct kern_ipc_perm *)*size +
-     sizeof(struct ipc_id_ary));
+ memcpy(new->p, ids->entries->p, sizeof(struct kern_ipc_perm *)*size);
  for(i=size;i<newsize;i++) {
   new->p[i] = NULL;
  }
```