Subject: [PATCH] fdset's leakage
Posted by Kirill Korotaev on Mon, 10 Jul 2006 13:40:51 GMT
View Forum Message <> Reply to Message

Andrew,

Another patch from Alexey Kuznetsov fixing memory leak in alloc_fdtable().

[PATCH] fdset's leakage

When found, it is obvious. nfds calculated when allocating fdsets
is rewritten by calculation of size of fdtable, and when we are
unlucky, we try to free fdsets of wrong size.

Found due to OpenVZ resource management (User Beancounters).

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

```
diff -urp linux-2.6-orig/fs/file.c linux-2.6/fs/file.c
--- linux-2.6-orig/fs/file.c 2006-07-10 12:10:51.000000000 +0400
+++ linux-2.6/fs/file.c 2006-07-10 14:47:01.000000000 +0400
@@ -277,11 +277,13 @@ static struct fdtable *alloc_fdtable(int
  } while (nfds <= nr);
  new_fds = alloc_fd_array(nfds);
  if (!new_fds)
-  goto out;
+  goto out2;
  fdt->fd = new_fds;
  fdt->max_fds = nfds;
  fdt->free_files = NULL;
  return fdt;
+out2:
+ nfds = fdt->max_fdset;
 out:
    if (new_openset)
     free_fdset(new_openset, nfds);
```