Subject: [PATCH ACPI] memory leakages in driver/acpi/video.c
Posted by vaverin on Sun, 09 Apr 2006 15:06:12 GMT
View Forum Message <> Reply to Message

Unlike my previously patches this one is not trivial and it is not tested
properly. I'm not an expert in ACPI-related questions therefore this patch may
be wrong.

Len, could you please check it carefully?

acpi_video_bus_get_one_device() and other functions in driver/acpi/video.c do
not release allocated memory on remove and on the error path.

Signed-off-by: Vasily Averin <vvs@sw.ru>

Thank you,
 Vasily Averin

SWsoft Virtuozzo/OpenVZ Linux kernel team

```
--- a/drivers/acpi/video.c 2006-03-20 08:53:29.000000000 +0300
+++ b/drivers/acpi/video.c 2006-04-09 18:34:38.000000000 +0400
@@ -1294,7 +1294,7 @@ acpi_video_bus_get_one_device(struct acp
         struct acpi_video_bus *video)
 {
  unsigned long device_id;
- int status, result;
+ int status;
  struct acpi_video_device *data;

  ACPI_FUNCTION_TRACE("acpi_video_bus_get_one_device");
@@ -1346,8 +1346,11 @@ acpi_video_bus_get_one_device(struct acp
   if (ACPI_FAILURE(status)) {
    ACPI_DEBUG_PRINT((ACPI_DB_ERROR,
        "Error installing notify handler\n"));
-   result = -ENODEV;
-   goto end;
+   if(data->brightness)
+    kfree(data->brightness->levels);
+   kfree(data->brightness);
+   kfree(data);
+   return_VALUE(-ENODEV);
   }

   down(&video->sem);
@@ -1358,8 +1361,6 @@ acpi_video_bus_get_one_device(struct acp

   return_VALUE(0);
```

```
 }
-
-     end:
 return_VALUE(-ENOENT);
}

@@ -1643,8 +1644,9 @@ static int acpi_video_bus_put_devices(st
    printk(KERN_WARNING PREFIX
          "hhuuhhuu bug in acpi video driver.\n");

+  if (data->brightness);
+   kfree(data->brightness->levels);
   kfree(data->brightness);
-
   kfree(data);
 }

@@ -1785,6 +1787,10 @@ static int acpi_video_bus_add(struct acp
 if (ACPI_FAILURE(status)) {
   ACPI_DEBUG_PRINT((ACPI_DB_ERROR,
       "Error installing notify handler\n"));
+  acpi_video_bus_stop_devices(video);
+  acpi_video_bus_put_devices(video);
+  kfree(video->attached_array);
+  acpi_video_bus_remove_fs(device);
   result = -ENODEV;
   goto end;
 }
@@ -1797,7 +1803,6 @@ static int acpi_video_bus_add(struct acp

      end:
 if (result) {
-  acpi_video_bus_remove_fs(device);
   kfree(video);
 }
```