author	Gaosheng Cui <cuigaosheng1@huawei.com>	2022-10-25 21:33:57 +0800
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2022-11-10 18:15:39 +0100
commit	2de8eec8afb75792440b8900a01d52b8f6742fd1 (patch)	
tree	ec782d047dd32aff1c2130dc88f529b96f9593e8	
parent	bd07f8067b35153190ad63e5174987e0a1335031 (diff)	
download	linux-2de8eec8afb75792440b8900a01d52b8f6742fd1.tar.gz	

diff options

context: 3

space: include

mode: unified

capabilities: fix potential memleak on error path from vfs_getxattr_alloc()

```
commit 8cf0a1bc12870d148ae830a4ba88cfdf0e879cee upstream.

In cap_inode_getsecurity(), we will use vfs_getxattr_alloc() to
complete the memory allocation of tmpbuf, if we have completed
the memory allocation of tmpbuf, but failed to call handler->get(...),
there will be a memleak in below logic:

  |-- ret = (int)vfs_getxattr_alloc(mnt_userns, ...)
    |           /* ^^^ alloc for tmpbuf */
    |-- value = krealloc(*xattr_value, error + 1, flags)
    |           /* ^^^ alloc memory */
    |-- error = handler->get(handler, ...)
    |           /* error! */
    |-- *xattr_value = value
    |           /* xattr_value is &tmpbuf (memory leak!) */

So we will try to free(tmpbuf) after vfs_getxattr_alloc() fails to fix it.

Cc: stable@vger.kernel.org
Fixes: 8db6c34f1dbc ("Introduce v3 namespaced file capabilities")
Signed-off-by: Gaosheng Cui <cuigaosheng1@huawei.com>
Acked-by: Serge Hallyn <serge@hallyn.com>
[PM: subject line and backtrace tweaks]
Signed-off-by: Paul Moore <paul@paul-moore.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r-- security/commoncap.c 6

1 files changed, 4 insertions, 2 deletions

```
diff --git a/security/commoncap.c b/security/commoncap.c
index 5fc8986c3c77cd..bc751fa5adad73 100644
--- a/security/commoncap.c
+++ b/security/commoncap.c
@@ -401,8 +401,10 @@ int cap_inode_getsecurity(struct user_namespace *mnt_userns,
                                        &tmpbuf, size, GFP_NOFS);
        dput(dentry);

-       if (ret < 0 || !tmpbuf)
-               return ret;
+       if (ret < 0 || !tmpbuf) {
```

```
+                size = ret;
+                goto out_free;
+        }

        fs_ns = inode->i_sb->s_user_ns;
        cap = (struct vfs_cap_data *) tmpbuf;
```