



index : kernel/git/stable/linux.git

Linux kernel stable tree

master

switch

Stable Group

[about](#) [summary](#) [refs](#) [log](#) [tree](#) [commit](#) [diff](#) [stats](#)

log msg

search

author Gaosheng Cui <cuigaosheng1@huawei.com> 2022-10-25 21:33:57 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 17:46:55 +0100
commit 90577bcc01c4188416a47269f8433f70502abe98 (patch)
tree 9127b1d9f786ea44c2afc60df6bba1145fa64522
parent d9142a9dd8a5d6703cc1897c6a60cc99cf8e2a83 (diff)
download linux-90577bcc01c4188416a47269f8433f70502abe98.tar.gz

diff options

context: 3
space: include
mode: unified

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

commit 8cf0a1bc12870d148ae830a4ba88cfd0e879cee 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 = kcalloc(*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 876cfe01d93914..28b204eacc7a30 100644

--- a/security/commoncap.c

+++ b/security/commoncap.c

@@ -397,8 +397,10 @@ int cap_inode_getsecurity(struct inode *inode, const char *name, void **buffer,
 &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;
```