author	Sean Heelan <seanheelan@gmail.com>	2025-04-07 11:26:50 +0000
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2025-04-25 10:45:48 +0200
commit	1db2451de23e98bc864c6a6e52aa0d82c91cb325 (patch)	
tree	2bf10df7851ca55ba31ad88d52d9bb3a2ee3c782	
parent	0874b629f65320778e7e3e206177770666d9db18 (diff)	
download	linux-1db2451de23e98bc864c6a6e52aa0d82c91cb325.tar.gz	

diff options

context: 3

space: include

mode: unified

ksmbd: Fix dangling pointer in krb_authenticate

```
commit 1e440d5b25b7efccb3defe542a73c51005799a5f upstream.

krb_authenticate frees sess->user and does not set the pointer
to NULL. It calls ksmbd_krb5_authenticate to reinitialise
sess->user but that function may return without doing so. If
that happens then smb2_sess_setup, which calls krb_authenticate,
will be accessing free'd memory when it later uses sess->user.

Cc: stable@vger.kernel.org
Signed-off-by: Sean Heelan <seanheelan@gmail.com>
Acked-by: Namjae Jeon <linkinjeon@kernel.org>
Signed-off-by: Steve French <stfrench@microsoft.com>
Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

Diffstat

-rw-r--r-- fs/smb/server/smb2pdu.c 4

1 files changed, 3 insertions, 1 deletions

```
diff --git a/fs/smb/server/smb2pdu.c b/fs/smb/server/smb2pdu.c
index 8877f9e900b2fb..d41d67ec5ee51a 100644
--- a/fs/smb/server/smb2pdu.c
+++ b/fs/smb/server/smb2pdu.c
@@ -1599,8 +1599,10 @@ static int krb5_authenticate(struct ksmbd_work *work,
        if (prev_sess_id && prev_sess_id != sess->id)
                destroy_previous_session(conn, sess->user, prev_sess_id);

-       if (sess->state == SMB2_SESSION_VALID)
+       if (sess->state == SMB2_SESSION_VALID) {
                ksmbd_free_user(sess->user);
+               sess->user = NULL;
+       }

        retval = ksmbd_krb5_authenticate(sess, in_blob, in_len,
                                         out_blob, &out_len);
```