

Thursday, November 8, 2018 2:01 PM

### User Scenario (In a nut shell)

- ### User Scenario (Details)

Asterisk 13 Upgrade Page 1

```
#10 0x00000000057b352 in __ast_pbx_run (c=0x7f2aa8bacdb0, args=0x0) at pbx.c:4288
#11 0x00000000057cd76 in pbx_thread (data=0x7f2aa8bacdb0) at pbx.c:4610
#12 0x000000000604421 in dummy_start (data=0x7f2aa8236da0) at utils.c:1238
#13 0x0000003802607aa1 in start_thread (arg=0x7f2a7054f700) at pthread_create.c:301
#14 0x00000038022e8bcd in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:115
```

### My research and thoughts and additional information

Looking at the code, it seems that 1 or more *roles* do exist and that *role\_options* for those roles do exist in the *roles datastore* of the channel. I am basing this on code entering the two AST\_LIST\_TRAVERSE code blocks in the ast\_bridge\_channel\_establish\_roles function of the bridge\_roles.c module.

I have put debug in the ast\_bridge\_channel\_establish\_roles function of bridge\_roles.c module as follows, in order to track down what I can. When a crash happened in this scenario, it crashed at the highlighted section below. I am assuming that Role\_option->option or Role\_option->value no longer are accessible.

```
.
.
.

AST_LIST_TRAVERSE(&roles_datastore->role_list, role, list) {
    struct bridge_role *this_role_copy;

    if (setup_bridge_role(bridge_channel->bridge_roles, role->role)) {
        /* We need to abandon the copy because we couldn't setup a role */
        ast_bridge_channel_clear_roles(bridge_channel);
        return -1;
    }
    this_role_copy = AST_LIST_LAST(&bridge_channel->bridge_roles->role_list);

    if (!this_role_copy)
        ast_debug(5, "JEFFBAD - copy of bridge role is null or empty. Channel: %s\n", ast_channel_name(bridge_channel->chan));

    if (role)
        ast_debug(5, "JEFFINFORM - Inside outside interaction of datastore. Role name: %s Channel: %s\n", role->role, ast_channel_name(bridge_channel->chan));
    else
        ast_debug(5, "JEFFBAD - Role is null or empty. Channel: %s\n", ast_channel_name(bridge_channel->chan));

    AST_LIST_TRAVERSE(&role->options, role_option, list) {

        if (!role_option)
        {
            ast_debug(5, "JEFFBAD - Role option is null or empty and the code following is expecting it not to be empty. Channel: %s\n", ast_channel_name(bridge_channel->chan));
        }
        else
        {
            Crash happens here (Role_option object exists, but the values option and value must be gone)

            ast_debug(5, "JEFFGOOD - Role option is %s Channel: %s\n", role_option->option, ast_channel_name(bridge_channel->chan));
            ast_debug(5, "JEFFGOOD - Role option value is %s Channel: %s\n", role_option->value, ast_channel_name(bridge_channel->chan));
        }

        if (setup_bridge_role_option(this_role_copy, role_option->option, role_option->value)) {
            /* We need to abandon the copy because we couldn't setup a role option */
            ast_bridge_channel_clear_roles(bridge_channel);
            return -1;
        }
    }
}
.
.
.
```

I have put my own debug in the Asterisk near the point of failure but it does not log the information in the debug file right at the crash time. I suspect that it crashed before it could process the calls to the debug log file.

