Closed · Issue created 2 years ago by Hanno Böck

Crash on malformed server response with minimal capabilities

evolution can crash with a null pointer access if it gets some malformed responses from the server. This requires a configuration with STARTTLS.

Here's a minimized example of a crashing imap session:

```
* OK x
A00000 CAPABILITY
A00000 OK [x]
A00001 STARTTLS
A00001 OK x
```

First, third and fifth line come from the server, this can be simulated with netcat (nc -l -p 143, setting imap server to localhost), only thing that needs to happen dynamically is that the A00000-prefix isn't static, this can be something else from the client.

This leads to a crash in imapx_free_capability, caused by this code in imapx_connect_to_server:

```
                    /* See if we got new capabilities
                     * in the STARTTLS response. */
                    imapx_free_capability (is->priv->cinfo);
```

I believe what happens here is that cinfo isn't filled in some situations and the code expects it to be filled and wants to free it after initializing a STARTTLS process.

Here's a crash report from asan:

```
==6994==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x7fa0a7b14f38 bp 0x000000000000 sp 0x7fa0a785f400 T5)
==6994==The signal is caused by a READ memory access.
==6994==Hint: address points to the zero page.
    #0 0x7fa0a7b14f37 in imapx_free_capability /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data-server-
    #1 0x7fa0a7aeebc2 in imapx_connect_to_server /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data-serve
    #2 0x7fa0a7afdafa in imapx_reconnect /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data-server-3.32.5
    #3 0x7fa0a7afdafa in camel_imapx_server_connect_sync /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-da
    #4 0x7fa0a7abac5f in imapx_create_new_connection_unlocked /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evoluti
    #5 0x7fa0a7abac5f in camel_imapx_conn_manager_ref_connection /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evol
    #6 0x7fa0a7abbafa in camel_imapx_conn_manager_connect_sync /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolut
    #7 0x7fa0a7b0dd10 in imapx_connect_sync /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data-server-3.3
    #8 0x7fa0b98d8cac in service_shared_connect_thread /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data
    #9 0x7fa0b8057171  (/usr/lib64/libgio-2.0.so.0+0xa2171)
    #10 0x7fa0b7eae713  (/usr/lib64/libglib-2.0.so.0+0x77713)
    #11 0x7fa0b7eadd2c  (/usr/lib64/libglib-2.0.so.0+0x76d2c)
    #12 0x7fa0b2e5d2d6 in start_thread /var/tmp/portage/sys-libs/glibc-2.30-r3/work/glibc-2.30/nptl/pthread_create.c:479
    #13 0x7fa0b2d8ba5e in __clone (/lib64/libc.so.6+0x106a5e)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /var/tmp/portage/gnome-extra/evolution-data-server-3.32.5/work/evolution-data-server-3.32.5/src/came
Thread T5 (pool-evolution) created by T0 here:
    #0 0x7fa0b9b3e211 in pthread_create (/usr/lib/gcc/x86_64-pc-linux-gnu/9.2.0/libasan.so.5+0x3a211)
    #1 0x7fa0b7ecfd32  (/usr/lib64/libglib-2.0.so.0+0x98d32)
```

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. More information

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Activity

Andre Klapper added 1. Crash label 2 years ago

Milan Crha @mcrha · 2 years ago · Maintainer

Thanks for a bug report. It seems it's the only place where the non-NULL check had been missing. I'm going to commit a change for it.

Milan Crha closed via commit 2cc39592 2 years ago

Milan Crha @mcrha · 2 years ago · Maintainer

The above commit is for 3.35.91+.

Please register or sign in to reply