Bug 4313 - Recursion stack overflow (two variations) with rebuilding folder tree

Status: RESOLVED FIXED

Alias: None

Product: Claws Mail (GTK 2)
Component: Folders/IMAP (show other bugs)
Version: 3.17.4
Hardware: PC Linux

Importance: P3 normal
Assignee: wwp

URL: https://cve.mitre.org/cgi-bin/cvename...

Depends on:
Blocks:

Reported: 2020-02-15 12:42 UTC by Hanno Boeck
Modified: 2020-09-29 12:04 UTC (History)
CC List: 1 user (show)

See Also:

Attachments		
python poc for first variant (977 bytes, text/x-python3) 2020-02-15 12:42 UTC, Hanno Boeck	*no flags*	Details
python poc for second variant (1.02 KB, text/x-python3) 2020-02-15 12:43 UTC, Hanno Boeck	*no flags*	Details
asan crash dump variant 1 (3.41 KB, text/plain) 2020-02-15 12:47 UTC, Hanno Boeck	*no flags*	Details
asan crash dump variant 2 (863 bytes, text/plain) 2020-02-15 12:48 UTC, Hanno Boeck	*no flags*	Details
patch candidate wwp-rev2 (3.23 KB, patch) 2020-08-29 18:18 UTC, wwp	*no flags*	Details | Diff
Add an attachment (proposed patch, testcase, etc.)		Show Obsolete (2)

Hanno Boeck 2020-02-15 12:42:48 UTC — Description

Created attachment 2046 [details]
python poc for first variant

A malicious or faulty IMAP server can crash claws-mail when it lets the server traverse into indefinitely many subdirectories during rebuild folder tree.

The source of this is relatively obvious: imap_scan_tree_recursive() will call itself recursively without any limit set, which eventually will crash. I recomend to set a reasonable limit of recursion depth (not sure how crazy people plausibly go with imap structures, but I guess a limit at 500 should handle all possibly legit needs).

However while trying to create a reproducer for this I noticed that when terminating the connection after some iterations (I tried with 1000) it will be unresponsive for a while and also cause a stack overflow, however a different one. It will crash somewhere in glib. I haven't analyzed that in more detail, but it seems the rebuild folder tree functionality doesn't detect the connection termination.

I'm attaching test scripts, these are written in python and open an imap server on localhost. Configure an imap account to localhost without tls and do rightclick->"Rebuild folder tree" to reproduce. I'm also attaching ASAN stack traces for both bugs.

Hanno Boeck 2020-02-15 12:43:07 UTC — Comment 1

Created attachment 2047 [details]
python poc for second variant

Hanno Boeck 2020-02-15 12:47:53 UTC — Comment 2

Created attachment 2048 [details]
asan crash dump variant 1

Hanno Boeck 2020-02-15 12:48:07 UTC — Comment 3

Created attachment 2049 [details]
asan crash dump variant 2

Ricardo Mones 2020-08-05 18:24:02 UTC — Comment 4

And also as Debian bug https://bugs.debian.org/966630

wwp 2020-08-25 11:48:56 UTC — Comment 5

Created ~~attachment 2080~~ ~~[details]~~
patch candidate wwp-rev0

Here's a patch candidate, that limits the IMAP rebuild folder tree recursion to 256 (hardcoded, arbitrary value).

wwp 2020-08-29 14:26:10 UTC — Comment 6

Created ~~attachment 2081~~ ~~[details]~~
patch candidate wwp-rev1

wwp 2020-08-29 18:18:04 UTC — Comment 7

Created attachment 2082 [details]
patch candidate wwp-rev2

this time with a hidden pref, depth limit set to 64

Hanno Boeck 2020-09-04 13:40:58 UTC — Comment 8

I have tested the patch and I still get somewhat undesired behavior.

I can confirm that it no longer crashes directly if I run against the poc.

however I did some testing where I first ran claws without this patch and then ran an asan build of the patched claws. This resulted in a stack overflow which looks like the variant 2 stack overflow.

What I suspect is happening here is that traversing through the locally cached copy of the folder tree can also lead to a stack overflow.

Now given the patch applied such a situation should no longer be possible to occur. However I guess it would also be desirable to avoid crashing on bad local imap data.

Hanno Boeck 2020-09-04 14:01:27 UTC Comment 9

You can also cause a stack overflow by using deeply nested local directories.
Simply create a deeply nested dir structure in a local mail directory:

```
for i in $(seq 1 1000); do mkdir a; cd a; done
```

Then do a "Rebuild Folder Tree".

Michael Schwendt 2020-09-29 11:49:29 UTC Comment 10

So, is 3.17.7 accepted as a fix for CVE-2020-16094 or not?

Paul 2020-09-29 12:04:29 UTC Comment 11

See https://git.claws-mail.org/?p=claws.git;a=commit;h=3acca60b6efd93f23607754305a9810b56b44efd

See RELEASE_NOTES

See the Status of this bug.

IOW: yes. (but who is doing the accepting in your question?)

Note

You need to log in before you can comment on or make changes to this bug.

Format For Printing - XML - Clone This Bug - Top of page