Packages - Bug #3625

pacman: segmentation fault

2024-04-16 12:07 PM - da

Status:	fixed	**% Done:**	0%
Priority:	bug		
Assignee:			
Category:			

Description

- steps to reproduce:
  1) "pacman -Syy" or "pacman -Suw".
- I expected system upgrade.
- actual result: segmentation fault after each download action, no matter db or package.

```
debug: pacman v6.1.0 - libalpm v14.0.0
debug: config: attempting to read file /etc/pacman.conf
debug: config: new section 'options'
debug: config: HoldPkg: pacman
debug: config: HoldPkg: glibc
debug: config: xfercommand: /usr/bin/curl -L -C - -f -o %o %u
debug: config: Architecture: x86_64
debug: config: arch: x86_64

debug: config: usesyslog
debug: config: SigLevel: Optional
debug: config: LocalFileSigLevel: Optional
debug: config: RemoteFileSigLevel: Optional
debug: config: new section 'nonprism'

debug: setup_libalpm called
debug: option 'logfile' = /var/log/pacman.log
debug: option 'gpgdir' = /etc/pacman.d/gnupg/
debug: option 'hookdir' = /etc/pacman.d/hooks/
debug: option 'cachedir' = /var/cache/pacman/pkg/

:: Starting full system upgrade...

Total Download Size:    446.35 MiB
Total Installed Size:  1758.63 MiB
Net Upgrade Size:         4.48 MiB

:: Proceed with installation? [Y/n] debug: using cachedir: /var/cache/pacman/pkg/
debug: checking available disk space for download
debug: discovered mountpoint: /sys/kernel/security
debug: discovered mountpoint: /sys/kernel/debug
debug: discovered mountpoint: /sys/kernel/config
debug: discovered mountpoint: /sys/fs/pstore
debug: discovered mountpoint: /sys/fs/cgroup/unified
debug: discovered mountpoint: /sys/fs/cgroup/rdma
debug: discovered mountpoint: /sys/fs/cgroup/pids
debug: discovered mountpoint: /sys/fs/cgroup/perf_event
debug: discovered mountpoint: /sys/fs/cgroup/openrc
debug: discovered mountpoint: /sys/fs/cgroup/net_prio
debug: discovered mountpoint: /sys/fs/cgroup/net_cls
debug: discovered mountpoint: /sys/fs/cgroup/misc
debug: discovered mountpoint: /sys/fs/cgroup/memory
debug: discovered mountpoint: /sys/fs/cgroup/hugetlb
debug: discovered mountpoint: /sys/fs/cgroup/freezer
debug: discovered mountpoint: /sys/fs/cgroup/devices
debug: discovered mountpoint: /sys/fs/cgroup/cpuset
```

```
debug: discovered mountpoint: /sys/fs/cgroup/cpuacct
debug: discovered mountpoint: /sys/fs/cgroup/cpu
debug: discovered mountpoint: /sys/fs/cgroup/blkio
debug: discovered mountpoint: /sys/fs/cgroup
debug: discovered mountpoint: /sys
debug: discovered mountpoint: /run/user/976
debug: discovered mountpoint: /run/user/0
debug: discovered mountpoint: /run
debug: discovered mountpoint: /proc/sys/fs/binfmt_misc
debug: discovered mountpoint: /proc
debug: discovered mountpoint: /home
debug: discovered mountpoint: /dev/shm
debug: discovered mountpoint: /dev/pts
debug: discovered mountpoint: /dev/mqueue
debug: discovered mountpoint: /dev
debug: discovered mountpoint: /boot
debug: discovered mountpoint: /
debug: loading fsinfo for /
debug: partition /, needed 114698, cushion 5121, free 33346972
:: Retrieving packages...
debug: running command: /usr/bin/curl -L -C - -f -o /var/cache/pacman/pkg/pcre2-10.43-3-x86_64.pkg
.tar.zst.part https://quantum-mirror.hu/mirrors/pub/parabola/core/os/x86_64/pcre2-10.43-3-x86_64.p
kg.tar.zst
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
  4 1511k    4 65297    0     0  71304      0  0:00:21 --:--:--  0:00:21 71284
 48 1511k   48  735k    0     0   385k      0  0:00:03  0:00:01  0:00:02  385k
 97 1511k   97 1471k    0     0   496k      0  0:00:03  0:00:02  0:00:01  496k
 97 1511k   97 1471k    0     0   371k      0  0:00:04  0:00:03  0:00:01  371k
100 1511k  100 1511k    0     0   345k      0  0:00:04  0:00:04 --:--:--  345k

error: segmentation fault
Please submit a full bug report with --debug if appropriate.
```

History

#1 - 2024-04-16 05:40 PM - bill-auger

- Description updated

- Subject changed from pacman segmentation fault. to pacman: segmentation fault

#2 - 2024-04-16 05:41 PM - bill-auger

- File deleted (pacman.txt.bz2)

#3 - 2024-04-16 05:47 PM - bill-auger

this is rather unusual - this would be very difficult to diagnose unless the bug is reproducible; but i doubt if anyone can reproduce it - if this was a general problem with pacman, many people would have complained about it already

does the same thing happen repeatedly? - if so, you can post a crash dump - also your log does not show which repos you have enabled - it is best to show the complete --debug output - you deleted large swaths of it

the output of `pacman -Qm` may also be interesting

#4 - 2024-04-17 08:43 AM - da

- File core.bz2 added

May be repeated.
Repos list no matter when fault occur on every download action.

```
(gdb) bt
#0  __pthread_kill_implementation (threadid=<optimized out>, signo=signo@entry=11, no_tid=no_tid@entry=0) at p
thread_kill.c:44
#1  0x00007d9387657393 in __pthread_kill_internal (signo=11, threadid=<optimized out>) at pthread_kill.c:78
#2  0x00007d93876066c8 in __GI_raise (sig=sig@entry=11) at ../sysdeps/posix/raise.c:26
#3  0x0000644a6f4ecc8f in segv_handler (signum=11) at ../src/pacman/sighandler.c:113
```

```
#4  <signal handler called>
#5  _alpm_download (handle=handle@entry=0x644a70344f30, payloads=payloads@entry=0x644a707cd8c0,
    localpath=localpath@entry=0x644a7035aa20 "/var/cache/pacman/pkg/") at ../lib/libalpm/dload.c:1045
#6  0x00007d9387891620 in _alpm_download (handle=handle@entry=0x644a70344f30, payloads=payloads@entry=0x644a70
7cd8c0,
    localpath=localpath@entry=0x644a7035aa20 "/var/cache/pacman/pkg/") at ../lib/libalpm/dload.c:1002
#7  0x00007d938789f07e in download_files (handle=0x644a70344f30) at ../lib/libalpm/sync.c:841
#8  _alpm_sync_load (handle=handle@entry=0x644a70344f30, data=data@entry=0x7ffd0c744c10) at ../lib/libalpm/syn
c.c:1233
#9  0x00007d93878a0db2 in alpm_trans_commit (handle=0x644a70344f30, data=data@entry=0x7ffd0c744c10) at ../lib/
libalpm/trans.c:188
#10 0x0000644a6f4edf11 in sync_prepare_execute () at ../src/pacman/sync.c:846
#11 0x0000644a6f4ee7d4 in sync_trans (targets=<optimized out>) at ../src/pacman/sync.c:738
#12 0x0000644a6f4e2064 in main (argc=<optimized out>, argv=0x7ffd0c744de8) at ../src/pacman/pacman.c:1283
(gdb)
```

#5 - 2024-04-17 09:33 PM - bill-auger

so this is the offending code:

```
int _alpm_download(alpm_handle_t *handle,
    alpm_list_t *payloads /* struct dload_payload */,
    const char *localpath)
{
  if(handle->fetchcb == NULL) {
....
  } else {
    alpm_list_t *p;
    int updated = 0;
    for(p = payloads; p; p = p->next) {
      struct dload_payload *payload = p->data;
      alpm_list_t *s;
      int ret = -1;

      if(payload->fileurl) {
....
      } else {
        for(s = payload->cache_servers; s && ret == -1; s = s->next) {
          ret = payload_download_fetchcb(payload, s->data, localpath);
        }
        for(s = payload->servers; s && ret == -1; s = s->next) {
          ret = payload_download_fetchcb(payload, s->data, localpath);
        }

        if (ret != -1 && payload->download_signature) {
          /* Download signature if requested */
          char *sig_fileurl;
          size_t sig_len = strlen(s->data) + strlen(payload->filepath) + 6; // <-- LOC 1045
```

without digging any deeper, it looks that the server URL is borked (presumably, one of s->data or payload->filepath is NULL) - i would check /etc/pacman.d/mirrorlist and /etc/pacman.conf very closely if you have modified them, merging any .pacnew files, etc

#6 - 2024-04-17 09:58 PM - bill-auger

just FWIW, i noticed that the latest code on the upstream master branch has a change in this code - maybe that is important

```
        for(s = payload->cache_servers; s; s = s->next) {
          ret = payload_download_fetchcb(payload, s->data, localpath);
          if (ret != -1) {
            goto download_signature;
          }
        }
        for(s = payload->servers; s; s = s->next) {
          ret = payload_download_fetchcb(payload, s->data, localpath);
          if (ret != -1) {
            goto download_signature;
          }
        }
download_signature:
        if (ret != -1 && payload->download_signature) {
```

could be ....
https://gitlab.archlinux.org/pacman/pacman/-/merge_requests/152

https://gitlab.archlinux.org/pacman/pacman/-/commit/eb5bf6913835e7553433ef82bdf0a456528f9b50

so also check if you have an 'XferCommand' defined in your /etc/pacman.conf, or if you have only one enabled remote repository URL

#7 - 2024-04-17 10:38 PM - bill-auger

- File arch-MR152.patch added

#8 - 2024-04-17 11:26 PM - da

Required and relevant files (except mirrorlist) may contain sensetive data. I will upload them and new core in encrypted form. I suggest to use "age" for this purpose. Otherwise I will modify them (if possible) before upload, but do not complain me then about missing some parts.

#9 - 2024-04-18 12:08 AM - bill-auger

you do not need to send anything more - i mentioned only pacman.conf and mirrorlist - neither of those would contain anything private; but i did not ask to see them, only that you should inspect them and merge any changes from .pacnew files - that is routine maintenance which every parabola user should know how to do

the most informative thing you could do now, is to ensure that your pacman.conf and mirrorlist are exactly the ones in the current 'pacman' and 'pacman-mirrorlist' packages, then try pacman again - if that makes the problem go away, then i can make a new pacman package applying the arch-MR152.patch, and ask you to try it with your customized pacman.conf and mirrorlist

#10 - 2024-04-18 01:16 AM - da

Relevant *.pacnew does not exists.

#11 - 2024-04-18 02:43 AM - bill-auger

unless you are prepared to debug this yourself, the only informative thing you could do now, is to ensure that your pacman.conf and mirrorlist are exactly the ones in the current 'pacman' and 'pacman-mirrorlist' packages - that is, pacman.conf and mirrorlist are *not* modified in any way - then try `pacman -Sw mc` again - if that downloads 'mc' properly, then i can make a new pacman package applying the arch-MR152.patch, and ask you to try it with your customized pacman.conf and mirrorlist

#12 - 2024-04-18 05:20 AM - oaken-source

note that strlen does not show up in the stack trace -- the fault occurs directly in libalpm. So either the strlen code was inlined completely (which is possible) or there might be an issue with the linkage of the C library.

this kind of issue could be triggered by a partial upgrade -- when was the last time you ran `pacman -Syu`? If you upgraded pacman manually without the rest of the system, then this could be the underlying issue.

#13 - 2024-04-18 05:45 AM - bill-auger

i noticed that too; but if 's' is NULL, the NULL pointer de-reference would happen in the outer scope while setting up the stack frame for strlen - if 's' was valid and 's->data' was NULL, NULL would be passed into strlen and the NULL pointer de-reference would happen in strlen, presuming that it was not in-lined

also note 'xfercommand' in the --debug log, which is a requisite for the upstream bug - so it is likely that da hit that bug

#14 - 2024-04-18 11:55 AM - da

I have discover that the bug can be reproduced ONLY when XferCommand option enabled. Even with default pacman.conf file.

Last system upgrade, including pacman, was at 2024-04-15. Usually I upgrade entire system, except a few irrelevant pieces listed in the IgnorePkg.

#15 - 2024-04-18 11:45 PM - bill-auger

da - plz try this pacman package with your XferCommand; and let us know if it works

```
# pacman -U https://repo.parabola.nu/pool/parabola/pacman-6.1.0-3.parabola2-x86_64.pkg.tar.zst
```

#16 - 2024-04-19 01:34 AM - da

Segmentation fault is gone.

#17 - 2024-04-19 01:52 AM - bill-auger

- Status changed from unconfirmed to fixed

ok i will consider one this fixed

Files

core.bz2	1.21 MB	2024-04-17	da

arch-MR152.patch	2.77 KB	2024-04-17	bill-auger