

AqBanking - Bug #250

segfault in n AB_Value_dup() when attempting SEPA transfer

16.12.2021 12:08 - mlenk

Status:	Closed	Beginn:	16.12.2021
Priorität:	Normal	Abgabedatum:	
Kategorie:	AqBanking	Anwendung:	aqbanking-cli
Betriebssystem:	Linux	Version der Anwendung:	
AqBanking-Version:	6.4.0		

Beschreibung

This is a bug report that was submitted via the Debian bug tracker
<https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1001708>

Package: libaqbanking44
Version: 6.4.0-1
Severity: normal

I'm using aqbanking / aqhbcI with HBIC chip card for 20 years now, and it has always worked rather fine in Debian, as far as I can remember.

However, recently, it stopped to work on Debian unstable (AqBanking 6.4.0), while the same configuration, account, data files and HBIC chip card continue to work smoothly on Debian 11 stable (AqBanking 6.2.10).

So this is a clear regression compared to Debian 11.

The error happens before there is any communication with either the bank or the HBIC chip card, merely while reading the CSV input file with SEPA transfers and building up some internal data structures prior to talking to the bank. /proc/fd for the proces shows only stdin/stdout/stderr.

```
$ gdb --args aqbanking-cli sepatransfers -a 663951200 -f /tmp/aqbanking_transfers_20211210.csv --p
rofile=sepatransfer
GNU gdb (Debian 10.1-2) 10.1.90.20210103-git
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
```

For help, type "help".
Type "apropos word" to search for commands related to "word"...

Reading symbols from aqbanking-cli...
Reading symbols from /usr/lib/debug/.build-id/65/920ab0c9608f4b8430b25f041ba00d1734afb9.debug...
(gdb) run

Starting program: /usr/bin/aqbanking-cli sepatransfers -a 663951200 -f /tmp/aqbanking_transfers_20211210.csv --profile=sepatransfer
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
__gmpn_copyi () at tmp-copyi.s:81
81 tmp-copyi.s: No such file or directory.
(gdb) bt
#0 __gmpn_copyi () at tmp-copyi.s:81
#1 0x00007ffff7db93f4 in AB_Value_dup (ov=0x555555605380) at ./src/libs/aqbanking/types/value.c:69
#2 0x00007ffff7da8b24 in AB_Transaction_dup (p_src=p_src@entry=0x5555556053f0)

```

at ./src/libs/aqbanking/types/transaction.c:771
#3 0x00007ffff7e2fc33 in AH_Job_TransferBase_HandleCommand_SepaUndated (j=0x5555555c72e0, t=0x5555556053f0)
at ./src/libs/plugins/backends/aqhbci/ajobs/jobtransferbase.c:524
#4 0x00007ffff7e931c3 in _addCommandToOutbox (outbox=0x5555555c4810, t=0x5555556053f0, a=0x555555b61780, u=0x5555555abf10,
pro=0x5555555f1ec0) at ./src/libs/plugins/backends/aqhbci/banking/provider_sendcmd.c:178
#5 _addCommandsToOutbox (ctx=0x5555555edba0, outbox=0x5555555c4810, uql=0x555555610920, pro=0x5555555f1ec0)
at ./src/libs/plugins/backends/aqhbci/banking/provider_sendcmd.c:245
#6 AH_Provider_SendCommands (pro=0x5555555f1ec0, pq=<optimized out>, ctx=0x5555555edba0)
at ./src/libs/plugins/backends/aqhbci/banking/provider_sendcmd.c:63
#7 0x00007ffff7d7a612 in _sendProviderQueues (pid=3, ctx=0x555555604990, pql=0x5555555b2370, ab=0x5555555abcb0)
at ./src/libs/aqbanking/banking_online.c:729
#8 _sendCommandsInsideProgress (pid=3, ctx=0x555555604990, commandList=<optimized out>, ab=0x5555555abcb0)
at ./src/libs/aqbanking/banking_online.c:578
#9 AB_Banking_SendCommands (ab=0x5555555abcb0, commandList=<optimized out>, ctx=0x555555604990)
at ./src/libs/aqbanking/banking_online.c:535
#10 0x000055555567e91 in execBankingJobs (ab=0x5555555abcb0, tList=0x555555598940, ctxFile=0x0)
at ./src/tools/aqbanking-cli/util.c:872
#11 0x00005555556a048 in sepaMultiJobs (ab=ab@entry=0x5555555abcb0, dbArgs=dbArgs@entry=0x5555555ab590, argc=argc@entry=6,
argv=argv@entry=0x7fffffffe5f0, multisepa_type=<optimized out>) at ./src/tools/aqbanking-cli/sepamultijobs.c:140
#12 0x000055555560ad6 in main (argc=6, argv=0x7fffffffe5f0) at ./src/tools/aqbanking-cli/main.c:395
(gdb) frame 1
#1 0x00007ffff7db93f4 in AB_Value_dup (ov=0x555555605380) at ./src/libs/aqbanking/types/value.c:69
69 mpq_set(v->value, ov->value);
(gdb) p *v
$1 = {_list1_element = 0x555555610e10, value = {{_mp_num = {_mp_alloc = 21845, _mp_size = 21845, _mp_d = 0x555555835ed0},
_mp_den = {_mp_alloc = 21845, _mp_size = 21845, _mp_d = 0x555555612e40}}}, currency = 0x0}
(gdb) p *ov
$2 = {_list1_element = 0x5555555f0ef0, value = {{_mp_num = {_mp_alloc = 1432425056, _mp_size = 21845,
_mp_d = 0x5555555f0ff0}, _mp_den = {_mp_alloc = 1432430912, _mp_size = 21845, _mp_d = 0x3}}}, currency = 0x0}
(gdb) frame 2
#2 0x00007ffff7da8b24 in AB_Transaction_dup (p_src=p_src@entry=0x5555556053f0)
at ./src/libs/aqbanking/types/transaction.c:771
771 p_struct->taxes=AB_Value_dup(p_src->taxes);
(gdb) p p_src->taxes
$3 = (AB_VALUE *) 0x555555605380
(gdb) p *p_src->taxes
$4 = {_list1_element = 0x5555555f0ef0, value = {{_mp_num = {_mp_alloc = 1432425056, _mp_size = 21845,
_mp_d = 0x5555555f0ff0}, _mp_den = {_mp_alloc = 1432430912, _mp_size = 21845, _mp_d = 0x3}}}, currency = 0x0}

(gdb) frame 12
#12 0x000055555560ad6 in main (argc=6, argv=0x7fffffffe5f0) at ./src/tools/aqbanking-cli/main.c:395
395 rv=sepaMultiJobs(ab, db, argc, argv, AQBANKING_TOOL_SEPA_DEBITNOTES);
(gdb) list
390 }
391 else if (strcasecmp(cmd, "sepaFlashDebitNote")==0) {
392 rv=sepaDebitNote(ab, db, argc, argv, 1);
393 }
394 else if (strcasecmp(cmd, "sepadebitnotes")==0) {
395 rv=sepaMultiJobs(ab, db, argc, argv, AQBANKING_TOOL_SEPA_DEBITNOTES);
396 }
397 else if (strcasecmp(cmd, "addtrans")==0) {
398 rv=addTransaction(ab, db, argc, argv);
399 }

```

```

(gdb) frame 11
#11 0x0000555555556a048 in sepaMultiJobs (ab=ab@entry=0x55555555abcb0, dbArgs=dbArgs@entry=0x55555555
ab590, argc=argc@entry=6,
argv=argv@entry=0x7fffffffe5f0, multisepa_type=<optimized out>) at ./src/tools/aqbanking-cli/sepam
ultijobs.c:140
140 rv=execBankingJobs(ab, jobList, ctxFile);
(gdb) list
135 if (dryRun) {
136 DBG_NOTICE(0, "Dry-run requested, not sending jobs");
137 writeJobsAsContextFile(jobList, ctxFile);
138 }
139 else {
140 rv=execBankingJobs(ab, jobList, ctxFile);
141 if (rv) {
142 DBG_ERROR(0, "Error on executeQueue (%d)", rv);
143 rvExec=3;
144 }
(gdb) frame 10
#10 0x00005555555567e91 in execBankingJobs (ab=0x55555555abcb0, tList=0x5555555598940, ctxFile=0x0)
at ./src/tools/aqbanking-cli/util.c:872
872 rv=AB_Banking_SendCommands(ab, tList, ctx);
(gdb) list
867 int rvExec=0;
868 AB_IMEXPORTER_CONTEXT *ctx=NULL;
869
870 /* execute job */
871 ctx=AB_ImExporterContext_new();
872 rv=AB_Banking_SendCommands(ab, tList, ctx);
873 if (rv) {
874 fprintf(stderr, "Error on executeQueue (%d)\n", rv);
875 rvExec=3;
876 }
(gdb) frame 9
#9 AB_Banking_SendCommands (ab=0x55555555abcb0, commandList=<optimized out>, ctx=0x5555555604990)
at ./src/libs/aqbanking/banking_online.c:535
535 rv=_sendCommandsInsideProgress(ab, commandList, ctx, pid);
(gdb) list
Undefined command: "lits". Try "help".
(gdb) list
530 0, /* no progress count */
531 0);
532 GWEN_Gui_ProgressLog(pid, GWEN_LoggerLevel_Notice, "AqBanking v"AQBANKING_VERSION_FULL_STRING)
;
533 GWEN_Gui_ProgressLog(pid, GWEN_LoggerLevel_Notice, I18N("Sending jobs to the bank(s)"));
534
535 rv=_sendCommandsInsideProgress(ab, commandList, ctx, pid);
536 AB_Banking_ClearCryptTokenList(ab);
537 if (rv) {
538 DBG_INFO(AQBANKING_LOGDOMAIN, "here (%d)", rv);
539 }

```

I don't have any idea about gmp, but to me the mp_alloc of 1432430912 on the source side looks quite large?

-- System Information:

Debian Release: bookworm/sid

APT prefers unstable-debug

APT policy: (500, 'unstable-debug'), (500, 'unstable')

Architecture: amd64 (x86_64)

Foreign Architectures: i386

Kernel: Linux 5.14.0-4-amd64 (SMP w/4 CPU threads)

Kernel taint flags: TAINT_DIE, TAINT_OOT_MODULE, TAINT_UNSIGNED_MODULE

Locale: LANG=en_US.UTF-8, LC_CTYPE=de_DE.UTF-8 (charmap=UTF-8), LANGUAGE not set

Shell: /bin/sh linked to /bin/bash

Init: systemd (via /run/systemd/system)

LSM: AppArmor: enabled

```
Versions of packages libaqbanking44 depends on:
ii libaqbanking-data 6.4.0-1
ii libc6 2.33-1
ii libgmp10 2:6.2.1+dfsg-3
ii libgwenhywfar79 5.7.4-1
ii libxml2 2.9.12+dfsg-5+b1
ii libxmlsec1 1.2.33-1+b1
ii zlib1g 1:1.2.11.dfsg-2

libaqbanking44 recommends no packages.

Versions of packages libaqbanking44 suggests:
ii aqbanking-tools 6.4.0-1

-- no debconf information
```

Historie

#1 - 16.12.2021 12:11 - mlenk

Second message forwarded from the Debian bug tracker:

misc correction: It's probably only about 10 years that I'm using aqbanking in this setup. In any case, it has been extremely stable for me during that time.

As for the actual bug: I built aqbanking 6.3.2 (from upstream git) on Debian unstable and the same problem can be observed there. I verified that the libaqbanking.so from the custom build is used in the process, so it's clearly not using the Debian-packaged library.

Same also is the case with upstream 6.1.0. Building 5.8.2 unfortunately fails as it expects gwenhywfar-config to be present, while the new version switched to pkg-config. Even after patching the autoconf, it's appears to be impossibel to build an old aqbanking5 against modern gwenhywfar, so I'm a bit lost.

#2 - 16.12.2021 12:13 - martin

- Status wurde von New zu In Progress geändert

Most likely already fixed in latest releases of Gwenhywfar and AqBanking.

#3 - 16.12.2021 12:18 - mlenk

Thanks, I'll package the new versions and ask the original submitter to re-test with the new versions.

#4 - 16.12.2021 12:21 - martin

- Status wurde von In Progress zu Feedback geändert

Thanks!!

BTW: I already am in contact with OP, waiting for updates. So I will change the status of this bug to "Feedback".

#5 - 16.12.2021 23:09 - martin

- Status wurde von Feedback zu Closed geändert

Fix confirmed.