New issue

Jump to bottom

DoS (Denial Of Service) Bug #1502

Closed cr0hn opened this issue on Dec 21, 2020 · 4 comments · Fixed by #1503

Labels bug

cr0hn commented on Dec 21, 2020

Bug impact

Redis Graph crashes and server downs

Bug explained

It's appear that Redis Graph doesn't processes well list of unknown data types. Typing this in the CLI, server crashes:

```
> GRAPH.QUERY "myGraph" "CYPHER A=[a]"
```

It also crashes with any invalid values in `A` .

Redis Bug report

```
=== REDIS BUG REPORT START: Cut & paste starting from here ===
1:M 16 Dec 2020 10:32:43.143 # Redis 6.0.5 crashed by signal: 11
1:M 16 Dec 2020 10:32:43.145 # Crashed running the instruction at: 0x7f926a6e3765
1:M 16 Dec 2020 10:32:43.145 # Accessing address: 0x10
1:M 16 Dec 2020 10:32:43.145 # Failed assertion: (:0)
```

```
------ STACK TRACE ------
EIP:
/usr/lib/redis/modules/redisgraph.so(+0x1b7765)[0x7f926a6e3765]
```

```
Backtrace:
redis-server *:6379(logStackTrace+0x32)[0x55e762d62e02]
redis-server *:6379(sigsegvHandler+0x9e)[0x55e762d634de]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x12730)[0x7f926b891730]
/usr/lib/redis/modules/redisgraph.so(+0x1b7765)[0x7f926a6e3765]
/usr/lib/redis/modules/redisgraph.so(AR_EXP_FromASTNode+0x6)[0x7f926a6e33c6]
/usr/lib/redis/modules/redisgraph.so(+0x1b7c7e)[0x7f926a6e3c7e]
/usr/lib/redis/modules/redisgraph.so(AR_EXP_FromASTNode+0x6)[0x7f926a6e33c6]
/usr/lib/redis/modules/redisgraph.so(+0x1b7c7e)[0x7f926a6e3c7e]
/usr/lib/redis/modules/redisgraph.so(AR_EXP_FromASTNode+0x6)[0x7f926a6e33c6]
/usr/lib/redis/modules/redisgraph.so(parse_params+0x140)[0x7f926a71e0b0]
/usr/lib/redis/modules/redisgraph.so(ExecutionCtx_FromQuery+0x1c)[0x7f926a6f080c]
/usr/lib/redis/modules/redisgraph.so(Graph_Query+0x48)[0x7f926a6f0ab8]
/usr/lib/redis/modules/redisgraph.so(+0x1fb5ad)[0x7f926a7275ad]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x7fa3)[0x7f926b886fa3]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x3f)[0x7f926b7b54cf]
```

```
------ INFO OUTPUT ------
```

Server

```
redis_version:6.0.5
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:a552bef8bac6cf1c
redis_mode:standalone
os:Linux 5.4.39-linuxkit x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:8.3.0
process_id:1
run_id:95e543fa2c07ff8ed405acb9a7ebe43a43377ea4
tcp_port:6379
uptime_in_seconds:5
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:14279243
executable:/data/redis-server
config_file:
```

Clients

```
connected_clients:1
client_recent_max_input_buffer:115242
client_recent_max_output_buffer:0
blocked_clients:1
tracking_clients:0
clients_in_timeout_table:0
```

Memory

```
used_memory:3399200
used_memory_human:3.24M
used_memory_rss:15708160
used_memory_rss_human:14.98M
used_memory_peak:3399200
used_memory_peak_human:3.24M
used_memory_peak_perc:100.14%
used_memory_overhead:947558
used_memory_startup:839632
used_memory_dataset:2451642
used_memory_dataset_perc:95.78%
allocator_allocated:3980560
allocator_active:4374528
allocator_resident:21929984
total_system_memory:2084671488
total_system_memory_human:1.94G
used_memory_lua:37888
used_memory_lua_human:37.00K
used_memory_scripts:0
used_memory_scripts_human:0B
number_of_cached_scripts:0
maxmemory:0
maxmemory_human:0B
maxmemory_policy:noeviction
allocator_frag_ratio:1.10
allocator_frag_bytes:393968
allocator_rss_ratio:5.01
allocator_rss_bytes:17555456
rss_overhead_ratio:0.72
rss_overhead_bytes:-6221824
mem_fragmentation_ratio:4.63
mem_fragmentation_bytes:12313848
mem_not_counted_for_evict:0
mem_replication_backlog:0
mem_clients_slaves:0
mem_clients_normal:107854
mem_aof_buffer:0
mem_allocator:jemalloc-5.1.0
active_defrag_running:0
lazyfree_pending_objects:0
```

Persistence

```
loading:0
rdb_changes_since_last_save:1
rdb_bgsave_in_progress:0
rdb_last_save_time:1608114758
rdb_last_bgsave_status:ok
rdb_last_bgsave_time_sec:-1
rdb_current_bgsave_time_sec:-1
rdb_last_cow_size:0
aof_enabled:0
aof_rewrite_in_progress:0
aof_rewrite_scheduled:0
aof_last_rewrite_time_sec:-1
aof_current_rewrite_time_sec:-1
aof_last_bgrewrite_status:ok
aof_last_write_status:ok
aof_last_cow_size:0
module_fork_in_progress:0
module_fork_last_cow_size:0
```

Stats

```
total_connections_received:1
total_commands_processed:3
instantaneous_ops_per_sec:1
total_net_input_bytes:206292
total_net_output_bytes:261
instantaneous_input_kbps:125.91
instantaneous_output_kbps:0.16
rejected_connections:0
sync_full:0
sync_partial_ok:0
sync_partial_err:0
expired_keys:0
expired_stale_perc:0.00
expired_time_cap_reached_count:0
expire_cycle_cpu_milliseconds:0
evicted_keys:0
keyspace_hits:4
keyspace_misses:1
pubsub_channels:0
pubsub_patterns:0
latest_fork_usec:0
migrate_cached_sockets:0
slave_expires_tracked_keys:0
active_defrag_hits:0
active_defrag_misses:0
active_defrag_key_hits:0
active_defrag_key_misses:0
tracking_total_keys:0
tracking_total_items:0
tracking_total_prefixes:0
unexpected_error_replies:0
```

Replication

```
role:master
connected_slaves:0
master_replid:6d0c230f73cf5b6fdde876088a417b5cc8b36533
master_replid2:0000000000000000000000000000000000000000
master_repl_offset:0
second_repl_offset:-1
repl_backlog_active:0
repl_backlog_size:1048576
repl_backlog_first_byte_offset:0
repl_backlog_histlen:0
```

CPU

```
used_cpu_sys:0.044293
used_cpu_user:0.224490
used_cpu_sys_children:0.005976
used_cpu_user_children:0.000929
```

Modules

```
module:name=graph,ver=20208,api=1,filters=0,usedby=[],using=[],options=[]
```

Commandstats

```
cmdstat_graph.QUERY:calls=3,usec=4510,usec_per_call=1503.33
```

Cluster

```
cluster_enabled:0
```

Keyspace

```
db0:keys=1,expires=0,avg_ttl=0

------ CLIENT LIST OUTPUT ------
id=6 addr=172.17.0.1:51154 fd=8 name= age=1 idle=0 flags=b db=0 sub=0 psub=0 multi=-1 qbuf=0 qbuf-free=90860 obl=0 oll=0 omem=0 events=r cmd=graph.QUERY user=default
```

```
------ REGISTERS ------
1:M 16 Dec 2020 10:32:43.158 #
RAX:0000000000000000 RBX:00007f926021f160
RCX:00007f926b89b360 RDX:00007f9269529ab0
RDI:00000000000000a0 RSI:0000000000000001
RBP:0000000000000050 RSP:00007f92695272f0
R8 :0000000000000008 R9 :000000000000009f
R10:0000000000000002 R11:00007f9269527f40
R12:0000000000000002 R13:00007f926b24d9f8
R14:0000000000000002 R15:0000000000000001
RIP:00007f926a6e3765 EFL:0000000000010206
CSGSFS:002b000000000033
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272ff) -> 00007f926ab5084e
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272fe) -> 00007f9269527390
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272fd) -> 00007f926a6e3c7e
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272fc) -> 00007f926021f1c0
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272fb) -> 00007f926a6e33c6
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272fa) -> 0000000000000001
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f9) -> 0000000000000002
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f8) -> 00007f926b24d9f8
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f7) -> 0000000000000002
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f6) -> 00007f926b21b690
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f5) -> 00007f926021f1c0
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f4) -> 00007f926adb3ba0
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f3) -> 00007f926021f1c0
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f2) -> 0000744e696c6f74
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f1) -> 00007f926ab5084e
1:M 16 Dec 2020 10:32:43.158 # (00007f92695272f0) -> 00007f9269527320

------ MODULES INFO OUTPUT ------
```

graph_executing commands

```
------ FAST MEMORY TEST ------
1:M 16 Dec 2020 10:32:43.159 # Bio thread for job type #0 terminated
1:M 16 Dec 2020 10:32:43.159 # Bio thread for job type #1 terminated
1:M 16 Dec 2020 10:32:43.160 # Bio thread for job type #2 terminated
*** Preparing to test memory region 55e762eae000 (2277376 bytes)
*** Preparing to test memory region 55e763bf0000 (270336 bytes)
*** Preparing to test memory region 7f9260000000 (4018176 bytes)
*** Preparing to test memory region 7f9265aa5000 (19398656 bytes)
*** Preparing to test memory region 7f9266d26000 (8388608 bytes)
*** Preparing to test memory region 7f9267527000 (8388608 bytes)
*** Preparing to test memory region 7f9267d28000 (8388608 bytes)
*** Preparing to test memory region 7f9268529000 (8388608 bytes)
*** Preparing to test memory region 7f9268d2a000 (8388608 bytes)
*** Preparing to test memory region 7f926952b000 (8388608 bytes)
*** Preparing to test memory region 7f9269d2c000 (8388608 bytes)
*** Preparing to test memory region 7f926adfd000 (12288 bytes)
*** Preparing to test memory region 7f926ae00000 (8388608 bytes)
*** Preparing to test memory region 7f926b6b8000 (16384 bytes)
*** Preparing to test memory region 7f926b879000 (24576 bytes)
*** Preparing to test memory region 7f926b89c000 (16384 bytes)
*** Preparing to test memory region 7f926bb85000 (16384 bytes)
*** Preparing to test memory region 7f926bdad000 (8192 bytes)
*** Preparing to test memory region 7f926bdda000 (4096 bytes)
.O.O.O.O.O.O.O.O.%
```

jeffreylovitz commented on Dec 21, 2020 Contributor

Hi **@cr0hn**,

Thanks for the report! This is an issue with the parameter processing logic - you try to access the alias `a`, which has not been introduced at this point. When you say you experienced the same with other invalid values, does that include anything that wasn't an unquoted string?

cr0hn commented on Dec 21, 2020 Author

Hi **@jeffreylovitz**,

Not really. All of then were unquoted string

jeffreylovitz commented on Dec 21, 2020 Contributor

Okay! we'll have a fix out shortly.

Unquoted strings will not currently be accepted properly as parameters, since we expect all parameters to resolve to constants, and an unquoted string is interpreted as a variable name.

jeffreylovitz mentioned this issue on Dec 21, 2020

Error on alias references in parameters #1503

Merged

gkorland added the bug label on Dec 22, 2020

swilly22 closed this as completed in #1503 on Dec 23, 2020

cr0hn commented on Jan 4, 2021 Author

I opened a CVE proposal for this bug:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35668

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Error on alias references in parameters
RedisGraph/RedisGraph

3 participants