New issue

Jump to bottom

# Null pointer dereferencing in dict.c and async.c #747

Closed **shouc** opened this issue on Jan 9, 2020 · 6 comments

**shouc** commented on Jan 9, 2020 • edited

The following code never aborts when `malloc` is unsuccessful, causing dereferencing of null pointers.

async.c:61

```
redisCallback *dup = malloc(sizeof(*dup));
memcpy(dup,src,sizeof(*dup)); // dup may be null
return dup;
```

dict.c:75

```
dict *ht = malloc(sizeof(*ht));
_dictInit(ht,type,privDataPtr); // ht may be null
```

dict.c:146

```
entry = malloc(sizeof(*entry));
entry->next = ht->table[index]; // entry may be null
```

dict.c:261

```
dictIterator *iter = malloc(sizeof(*iter));
iter->ht = ht; // iter may be null
```

**shouc** changed the title ~~Several potential null pointer dereferencing~~ Several null pointer dereferencing in dict.c and async.c on Jan 9, 2020

**shouc** changed the title ~~Several null pointer dereferencing in dict.c and async.c~~ Null pointer dereferencing in dict.c and async.c on Jan 9, 2020

**lamby** commented on Jan 19, 2020 Contributor

This has been given the CVE ID CVE-2020-7105.

**lamby** added a commit to lamby/hiredis that referenced this issue on Jan 19, 2020

`Abort if malloc() was unsuccessful. (Closes: redis#747)` 78cec25

**lamby** mentioned this issue on Jan 19, 2020

**CVE-2020-7105: Abort if malloc() was unsuccessful** #752

Closed

**michael-grunder** commented on Jan 19, 2020 Collaborator

We have an open PR that has this specific change in it along with a few other NULL pointer deref fixes although it does not immediately abort on failure to reallocate.

Just adding it here for reference.

**shouc** commented on Jan 19, 2020 • edited Author

fixed in #752 & #638, more is specified in #751

**shouc** closed this as completed on Jan 19, 2020

**lamby** commented on Jan 19, 2020 Contributor

Shall we close #752 as well then? I'm a little lost, especially as #638 has a bunch of other changes that will be very difficult to backport to older, released, versions of hiredis.

**lamby** added a commit to lamby/hiredis that referenced this issue on Jan 19, 2020

`Abort if malloc() was unsuccessful. (Closes: redis#747, redis#751)` dcc7cea

**michael-grunder** commented on Jan 19, 2020 Collaborator

Apologies, I wasn't trying to confuse the situation. I just wanted to mention that #638 contains the same change (in addition to many more changes).

Merging #752 now and then #638 later seems reasonable to me.

**shouc** commented on Jan 19, 2020 — Author

#752 contains more fixes on nullptr dereferencing so I also think merging these two is reasonable

2

**michael-grunder** added a commit to michael-grunder/hiredis that referenced this issue on Jan 20, 2020

`Safe allocation wrappers where we don't handle OOM` ··· `dfdc85a`

**lamby** added a commit to lamby/hiredis that referenced this issue on Jan 22, 2020

`Abort if malloc() was unsuccessful. (Closes: redis#747, redis#751)` `3e2ddf9`

**michael-grunder** added a commit that referenced this issue on Jan 22, 2020

`Rename allocation wrappers and add license info` ··· `70e73a3`

**michael-grunder** added a commit that referenced this issue on Jan 28, 2020

`Safe allocation wrappers (#754)` ··· `669ac9d`

**michael-grunder** added a commit that referenced this issue on Mar 12, 2020

`Safe allocation wrappers (#754)` ··· `a153788`

**valentinogeron** pushed a commit to valentinogeron/hiredis that referenced this issue on Mar 17, 2020

`Safe allocation wrappers (redis#754)` ··· `5a3a817`

**bjosv** mentioned this issue on Dec 7, 2020

**Vulnerability report affecting hiredis-vip** vipshop/hiredis-vip#136

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants