

batman-adv - Bug #136

check hash_add fail

12/30/2009 02:30 AM - Simon Wunderlich

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Simon Wunderlich	% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:	2012.0.0		
Description			
if hash_add fails (e.g. because kcalloc() for the bucket fails), references to data to be hashed may be lost. This might lead to memory leaks. There are still some cases for this behaviour, e.g. in translation-table.c (current revision: r1518)			

History

#1 - 03/26/2011 09:24 PM - Anonymous

- Assignee deleted (Anonymous)
- Category set to 2

#2 - 05/15/2011 11:55 AM - Anonymous

- % Done changed from 0 to 70
- Assignee set to Simon Wunderlich

hash_add now doesn't allocate memory anymore. Thus it is not possible to leak memory in that function after commit:4c4236064501e85915087f00a370df8d9f43028d - but the function still may fail and we have to check that in the calling function.

#3 - 11/01/2011 11:35 AM - Simon Wunderlich

it is not yet checked everywhere - we miss the check in translation-table.c at two points.

#4 - 07/01/2012 12:13 PM - Antonio Quartulli

- % Done changed from 70 to 90

After Simon's commit c2e935f5da562f008f77bb12995ebc10705cb15a also the two hash_add() invocations in translation-table.c are now checked.

#5 - 07/01/2012 10:36 PM - Simon Wunderlich

nice. as far as I see, what we don't handle yet ist:

- out of memory in originator.c / batadv_orig_hash_add_if() - we leave orig table in bad shape, also the return code is never checked.

Apart from that, I can't find any other unchecked usages of batadv_hash_add()

#6 - 07/01/2012 10:53 PM - Simon Wunderlich

Simon Wunderlich wrote:

nice. as far as I see, what we don't handle yet ist:

- out of memory in originator.c / batadv_orig_hash_add_if() - we leave orig table in bad shape, also the return code is never checked.

Apart from that, I can't find any other unchecked usages of batadv_hash_add()

well, I've just sent a patch for that (although it is not completely related, it just coincides to have hash_add in the name).

@Antonio, @Sven, I'd suggest to close the ticket now?

#7 - 07/01/2012 10:54 PM - Simon Wunderlich

- % Done changed from 90 to 100

- Status changed from New to Resolved

#8 - 08/07/2012 07:13 PM - Simon Wunderlich

- Status changed from Resolved to Closed

#9 - 02/11/2017 09:39 AM - Sven Eckelmann

- Target version set to 2012.0.0