

batman-adv - Bug #240

Bug # 235 (Closed): meta: Missing list checks for *list_add*

batadv_nc_get_nc_node: Missing list checks for *list_add*

03/05/2016 09:31 AM - Sven Eckelmann

Status:	Closed	Start date:	06/26/2015
Priority:	Normal	Due date:	
Assignee:	Martin Hundebøll	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	2018.3		

Description

Simon debugged the refcnt problem and submitted some patches to fix them. I had a brief look and noticed that there are possible more problems similar to the *list_del* ones - just with *list_add*. Basically some functions use some kind of get function, notice that the element does not exist and then create a new one to add to the list. Only the "list_add" is protected. The result may be that an element in twice in a list when only a single occurrence is allowed.

The problem I saw is that functions adding objects in an RCU protected list are missing an definitive check. They first call some kind of *_get (rcu_read_lock only) to check if an object with this value already exists and then uses some kind of *_add to allocate a new object and add it (which may already be added in by a different context). So it has to be made sure that nothing modifies the list between the check and the add of the new object).

History

#1 - 08/12/2018 09:07 PM - Sven Eckelmann

- Status changed from New to In Progress

See <https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/20180812190445.28013-3-sven@narfation.org/>

#2 - 09/08/2018 08:39 AM - Sven Eckelmann

- Target version set to 2018.3

- Status changed from In Progress to Resolved

Queued up for 2018.3

#3 - 09/14/2018 05:44 PM - Sven Eckelmann

- Status changed from Resolved to Closed