batctl - Bug #298

tcpdump: leak of dump_if on errors

10/19/2016 09:27 AM - Sven Eckelmann

Status:	Closed	**Start date:**	10/19/2016
Priority:	Low	**Due date:**	
Assignee:	Sven Eckelmann	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2017.0		

Description

Coverity reported following problem

```
1 new defect(s) introduced to batctl found with Coverity Scan.

New defect(s) Reported-by: Coverity Scan
Showing 1 of 1 defect(s)

** CID 153451:  Resource leaks  (RESOURCE_LEAK)
/tcpdump.c: 1304 in tcpdump()

________________________________________________________________________________
_____
*** CID 153451:  Resource leaks  (RESOURCE_LEAK)
/tcpdump.c: 1304 in tcpdump()
1298                            fflush(stdout);
1299                    }
1300
1301            }
1302
1303    out:
>>> CID 153451:  Resource leaks  (RESOURCE_LEAK)
>>> Overwriting "dump_if" in "dump_if = ({...})" leaks the storage that "dump_if" points to.
1304            list_for_each_entry_safe(dump_if, dump_if_tmp, &dump_if_list, list) {
1305                    if (dump_if->raw_sock >= 0)
1306                            close(dump_if->raw_sock);
1307
1308                    list_del(&dump_if->list);
1309                    free(dump_if);
```

Looks like the problem is not this cleanup loop. Instead it is about a dump_if which is not completely initialized (and thus not part of this list) and then a different error happend which caused a goto to this cleanup routine. The pointer to the allocated dump_if is then overwritten by list_for_each_entry_safe without the memory of it being freed.

History

#1 - 01/22/2017 01:08 PM - Sven Eckelmann

- Status changed from New to In Progress

Patch is queued up in https://patchwork.open-mesh.org/project/b.a.t.m.a.n./patch/20170122120749.27932-1-sven@narfation.org/

#2 - 02/10/2017 11:02 PM - Sven Eckelmann

- Status changed from In Progress to Resolved

Patch applied in https://git.open-mesh.org/batctl.git/commit/dfe9da9a567bc754c17d89dac3324dc1d2c4950f

#3 - 02/11/2017 12:23 AM - Sven Eckelmann

- Target version set to 2017.0

#4 - 02/11/2017 05:55 PM - Sven Eckelmann

- Assignee set to Sven Eckelmann

#5 - 02/28/2017 05:44 PM - Sven Eckelmann

- Status changed from Resolved to Closed