

batman-adv - Bug #227

Lock not held while in batadv_tvlv_container_remove

12/15/2015 04:56 PM - Heiko Wundram

Status:	Closed	Start date:	12/15/2015
Priority:	Low	Due date:	
Assignee:	Marek Lindner	% Done:	0%
Category:		Estimated time:	0.00 hour
Target version:	2016.0		
Description			
On an ARMv7l system, I'm seeing the following error while using batman-adv 2015.2:			
<pre>Dec 15 14:19:57 gw kernel: [c1] -----[cut here]----- Dec 15 14:19:57 gw kernel: [c1] WARNING: at /var/lib/dkms/batman-adv/2015.2/build/net/batman-adv/main.c:750 batadv_tvlv_container_remove+0x94/0xa0 [batman_adv]() Dec 15 14:19:57 gw kernel: [c1] Modules linked in: 8021q garp mrp bridge stp llc ip6table_filter ip6table_nat nf_conntrack_ipv6 nf_defrag_ipv6 nf_nat_ipv6 ip6table_mangle ip6_tables xt_hashlimit xt_multiport xt_conntrack iptable_filter cdc_ether xt_TCPMSS usbnet r8152 xt_tcpmss iptable_mangle iptable_nat nf_conntrack_ipv4 nf_defrag_ipv4 nf_nat_ipv4 nf_nat nf_conntrack ip_tables spi_s3c64xx ipcomp batman_adv(O) Dec 15 14:19:57 gw kernel: [c1] CPU: 1 PID: 2818 Comm: kworker/u16:0 Tainted: G W O 3.10.9-2-64 #1 Dec 15 14:19:57 gw kernel: [c1] Workqueue: bat_events batadv_send_outstanding_bat_ogm_packet [batman_adv] Dec 15 14:19:57 gw kernel: [c1] Backtrace: Dec 15 14:19:57 gw kernel: [c1] [<c0012da4>] (dump_backtrace+0x0/0x114) from [<c0013014>] (show_stack+0x20/0x24) Dec 15 14:19:57 gw kernel: [c1] r7:000002ee r6:bf01d340 r5:00000009 r4:00000000 Dec 15 14:19:57 gw kernel: [c1] [<c0012ff4>] (show_stack+0x0/0x24) from [<c05fc4d0>] (dump_stack+0x24/0x28) Dec 15 14:19:57 gw kernel: [c1] [<c05fc4ac>] (dump_stack+0x0/0x28) from [<c002b4bc>] (warn_slowpath_common+0x64/0x7c) Dec 15 14:19:57 gw kernel: [c1] [<c002b458>] (warn_slowpath_common+0x0/0x7c) from [<c002b590>] (warn_slowpath_null+0x2c/0x34) Dec 15 14:19:57 gw kernel: [c1] r9:de29ea50 r8:00000001 r7:00000004 r6:00001c00 r5:de29e5c0\0ar4:dcb68540 Dec 15 14:19:57 gw kernel: [c1] [<c002b564>] (warn_slowpath_null+0x0/0x34) from [<bf00c08c>] (batadv_tvlv_container_remove+0x94/0xa0 [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] [<bf00bff8>] (batadv_tvlv_container_remove+0x0/0xa0 [batman_adv]) from [<bf00cc8c>] (batadv_tvlv_container_register+0xa8/0xf8 [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] r5:de29e5c0 r4:dcb68280 Dec 15 14:19:57 gw kernel: [c1] [<bf00cbe4>] (batadv_tvlv_container_register+0x0/0xf8 [batman_adv]) from [<bf0177d4>] (batadv_tt_tvlv_container_update+0x190/0x1cc [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] [<bf017644>] (batadv_tt_tvlv_container_update+0x0/0x1cc [batman_adv]) from [<bf018200>] (batadv_tt_local_commit_changes_nolock+0x374/0x394 [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] [<bf017e8c>] (batadv_tt_local_commit_changes_nolock+0x0/0x394 [batman_adv]) from [<bf01b960>] (batadv_tt_local_commit_changes+0x30/0x3c [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] [<bf01b930>] (batadv_tt_local_commit_changes+0x0/0x3c [batman_adv]) from [<bf001308>] (batadv_iv_ogm_schedule+0x380/0x3b4 [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] r5:de29e000 r4:de29e5c0 Dec 15 14:19:57 gw kernel: [c1] [<bf000f88>] (batadv_iv_ogm_schedule+0x0/0x3b4 [batman_adv]) from [<bf013514>] (batadv_send_outstanding_bat_ogm_packet+0xf0/0x100 [batman_adv]) Dec 15 14:19:57 gw kernel: [c1] [<bf013424>] (batadv_send_outstanding_bat_ogm_packet+0x0/0x100 [batman_adv]) from [<c004a760>] (process_one_work+0x1b0/0x578) Dec 15 14:19:57 gw kernel: [c1] r7:dd391200 r6:df019c00 r5:dd010680 r4:dd29dc20 Dec 15 14:19:57 gw kernel: [c1] [<c004a5b0>] (process_one_work+0x0/0x578) from [<c004ac64>] (worker_thread+0x13c/0x3c8) Dec 15 14:19:57 gw kernel: [c1] [<c004ab28>] (worker_thread+0x0/0x3c8) from [<c0051a7c>] (kthread+0xc4/0xc8) Dec 15 14:19:57 gw kernel: [c1] [<c00519b8>] (kthread+0x0/0xc8) from [<c000e820>] (ret_from_fork+0x14/0x20) Dec 15 14:19:57 gw kernel: [c1] r7:00000000 r6:00000000 r5:c00519b8 r4:dd97fe14</pre>			

```
Dec 15 14:19:57 gw kernel: [c1] ---[ end trace bde3526140ca6de6 ]---
```

This error repeats every five seconds, but does not seem to impact stability of the system as a whole. The running system is:

```
Linux gw 3.10.92-64 #1 SMP PREEMPT Mon Nov 23 15:13:42 BRST 2015 armv7l armv7l armv7l GNU/Linux
```

(i.e. the default kernel for an XU3 system), and uses the module as a DKMS built with the standard debian DKMS-infrastructure.

History

#1 - 12/16/2015 09:26 AM - Sven Eckelmann

- *Project changed from alfred to batman-adv*

This is the wrong issue tracker. I've moved it now for you to batman-adv

#2 - 12/16/2015 09:27 AM - Sven Eckelmann

- *Status changed from New to Feedback*

Looks like a bug which was fixed a while ago (but for some reason not added to the 2015.2 release):

<https://git.open-mesh.org/batman-adv.git/patch/41a559a1d48b6fbb17690b7bdcc155668a8e751d>

Please test this patch

#3 - 12/16/2015 10:02 AM - Heiko Wundram

Sven Eckelmann wrote:

Looks like a bug which was fixed a while ago (but for some reason not added to the 2015.2 release):

<https://git.open-mesh.org/batman-adv.git/patch/41a559a1d48b6fbb17690b7bdcc155668a8e751d>

independently of that patch in trunk (which I didn't see), I did the same adaptation yesterday, and that fixes the problem. Would you kindly integrate the patch into the 2015.2 release-tar? Thanks!

#4 - 12/16/2015 10:37 PM - Sven Eckelmann

- *Priority changed from Normal to Low*

- *Assignee set to Marek Lindner*

Would you kindly integrate the patch into the 2015.2 release-tar?

No. 2015.2 is tagged, released as tarball, cryptographically signed, mirrored to other servers (not in our control) since a while and should never be modified again. This could only be released as a maintenance release like 2015.2.1 or as the next full release 2016.0. This is something which Marek

+ Simon have to decide. I doubt that it will be done because this is just a minor problem. It is only a warning from a debug helper of the kernel and it is not reporting an actual problem in the code. The mistake is only inside an annotation which is checked by the lockdep helper for debugging reasons.

Other question: why is your distribution kernel compiled with CONFIG_LOCKDEP? This is meant only for debug kernels (this is also the reason why this feature depends on CONFIG_DEBUG_KERNEL && CONFIG_LOCKDEP_SUPPORT)

#5 - 12/16/2015 10:48 PM - Sven Eckelmann

And btw. this patch is not in trunk (there is no trunk branch). It is currently in the next branch - which is the branch that will be used to prepare the 2016.0 release and is currently submitted by Antonio to the Linux kernel networking maintainer for 4.5. So they already decided that it is not interesting enough for the maint branch (which contains the patches for a potential v2015.2.1 and Linux 4.4).

#6 - 12/16/2015 11:17 PM - Heiko Wundram

Sven Eckelmann wrote:

No. 2015.2 is tagged, released as tarball, cryptographically signed, mirrored to other servers (not in our control) since a while and should never be modified again. This could only be released as a maintenance release like 2015.2.1 or as the next full release 2016.0. This is something which Marek + Simon have to decide. I doubt that it will be done because this is just a minor problem. It is only a warning from a debug helper of the kernel and it is not reporting an actual problem in the code. The mistake is only inside an annotation which is checked by the lockdep helper for debugging reasons.

Makes sense, absolutely, and I actually meant putting up a maintenance release as a "fix", as:

Other question: why is your distribution kernel compiled with CONFIG_LOCKDEP? This is meant only for debug kernels (this is also the reason why this feature depends on CONFIG_DEBUG_KERNEL && CONFIG_LOCKDEP_SUPPORT)

for the corresponding hardware, the kernel is the default kernel you'll find on new installation images of the XU3 platform, see http://www.hardkernel.com/main/products/prdt_info.php?g_code=G140448267127 (kernel from http://odroid.com/dokuwiki/doku.php?id=en:xu3_building_kernel) - and yes, it does have CONFIG_LOCKDEP turned on by default, seemingly, so that I won't be the only one being bitten and/or confused by this.

Functionality-wise: as of the present state, it spams the logs full of backtraces, which is annoying, but doesn't really break things except using up storage space for the sys-logs.

#7 - 01/20/2016 09:21 AM - Sven Eckelmann

- Status changed from Feedback to Closed

v2016.0 was now released with the mentioned patches

#8 - 02/11/2017 08:43 AM - Sven Eckelmann

- Target version set to 2016.0