strongSwan - Issue #2345

Crash in ha_ike hook_message

30.05.2017 11:38 - Avinoam Meir

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	libcharon		
Affected version:	5.3.2	**Resolution:**	Duplicate

Description

Hello,

I see several crashes with the same pattern.
Here is the stack:

```
     message_hook
         message_hook
         message
         generate_message
         generate_message_fragmented
         generate_message.isra.11
         process_message
         process_message
         execute
         process_jobs
    @     thread_main
```

In all the crashes that I investigated the logs looks like this:

STRONGSWAN ENC L_CTRL [vpn_x.x.x.x]: parsed CREATE_CHILD_SA request 5868 [SA No KE]
STRONGSWAN IKE L_AUDIT [vpn_x.x.x.x]: x.x.x.x is initiating an IKE_SA
STRONGSWAN IKE L_CTRL [vpn_x.x.x.x]: DH group MODP_1024 inacceptable, requesting MODP_2048

Seems that in this flow ,somehow the ike_sa of the thread gets lost,
Any idea why?

Thanks.

Related issues:

Is duplicate of Bug #862: strongswan server core! during IKE_SA rekeying	**Closed**	**25.02.2015**

History

#1 - 30.05.2017 11:39 - Avinoam Meir

I forgat to add that from reading the assembly I believe that message_hook (in ha_ike.c) was called with ike_sa=NULL.

#2 - 30.05.2017 14:05 - Tobias Brunner

- Is duplicate of Bug #862: strongswan server core! during IKE_SA rekeying added

#3 - 20.09.2018 18:25 - Tobias Brunner

- Status changed from New to Closed

- Resolution set to Duplicate