strongSwan - Bug #862

strongswan server core! during IKE_SA rekeying

25.02.2015 04:33 - richard hu

Status:	Closed	**Start date:**	25.02.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.3		
Affected version:	5.2.2	**Resolution:**	Fixed

Description

one of our strongswan server cored suddenly, although this is a issue that not happen very often, I still hope you guys can give some advice based on following information.
Is this a bug?

```
Feb 21 17:39:57 15[IKE] <IKEv2_EAP_RSA|1623534> DH group MODP_2048 inacceptable, requesting MODP_1
024
Feb 21 17:39:57 15[DMN] thread 15 received 11
Feb 21 17:39:57 15[LIB]  dumping 13 stack frame addresses:
Feb 21 17:39:57 15[LIB]  /lib/x86_64-linux-gnu/libpthread.so.0 @ 0x7f42562f0000 [0x7f42562ffcb0]
Feb 21 17:39:57 15[LIB]    -> ??:0
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/plugins/libstrongswan-eap-radius.so @ 0x7f4250b5d000 [0x7f
4250b62973]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/plugins/eap_radius/eap_radius_ac
counting.c:630
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f4256517b6d]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/bus/bus.c:556
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f425653639b]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/sa/ike_sa.c:1018
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f4256536492]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/sa/ike_sa.c:1068
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f4256540834]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/sa/ikev2/task_manager_v2.c:286
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f4256542001]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/sa/ikev2/task_manager_v2.c:813
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f42565366af]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/sa/ike_sa.c:1362
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libcharon.so.0 @ 0x7f425650d000 [0x7f42565309c7]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libcharon/processing/jobs/process_message_
job.c:74
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libstrongswan.so.0 @ 0x7f425698c000 [0x7f42569b87e3]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libstrongswan/processing/processor.c:235
Feb 21 17:39:57 15[LIB]  /usr/lib/ipsec/libstrongswan.so.0 @ 0x7f425698c000 [0x7f42569c8670]
Feb 21 17:39:57 15[LIB]    -> /home/adam/strongswan/src/libstrongswan/threading/thread.c:313
Feb 21 17:39:57 15[LIB]  /lib/x86_64-linux-gnu/libpthread.so.0 @ 0x7f42562f0000 [0x7f42562f7e9a]
Feb 21 17:39:57 15[LIB]    -> ??:0
Feb 21 17:39:57 15[LIB]  /lib/x86_64-linux-gnu/libc.so.6 @ 0x7f4255f31000 (clone+0x6d) [0x7f425602
52ed]
Feb 21 17:39:57 15[LIB]    -> ??:0
Feb 21 17:39:57 15[DMN] killing ourself, received critical signal
Feb 21 17:40:13 00[DMN] Starting IKE charon daemon (strongSwan 5.2.2, Linux 3.2.0-75-virtual, x86_
64)
```

Related issues:

Has duplicate Issue #918: ikev2 crash	**Closed**	**02.04.2015**
Has duplicate Issue #2345: Crash in ha_ike hook_message	**Closed**	

Associated revisions

Revision 86d20b0b - 27.07.2015 14:44 - Tobias Brunner

ike-rekey: Reset IKE_SA on the bus after destroying new IKE_SA

The destroy() method sets the IKE_SA on the bus to NULL, we reset it to the current IKE_SA so any events and log messages that follow happen in the correct context.

A practical example where this is problematic is a DH group mismatch, which causes the first CREATE_CHILD_SA exchange to fail. Because the SA was not reset previously, the message() hook for the CREATE_CHILD_SA response, for instance, was triggered outside the context of an IKE_SA, that is, the ike_sa parameter was NULL, which is definitely not expected by several plugins.

Fixes #862.

History

#1 - 05.03.2015 17:35 - Tobias Brunner

- Tracker changed from Bug to Issue

- Description updated

- Status changed from New to Feedback

- Assignee deleted (Martin Willi)

- Priority changed from Urgent to Normal

```
Feb 21 17:39:57 15[DMN] thread 15 received 11
Feb 21 17:39:57 15[LIB] dumping 13 stack frame addresses:
Feb 21 17:39:57 15[LIB] /lib/x86_64-linux-gnu/libpthread.so.0 0x7f42562f0000 [0x7f42562ffcb0]
Feb 21 17:39:57 15[LIB] -> ??:0
Feb 21 17:39:57 15[LIB] /usr/lib/ipsec/plugins/libstrongswan-eap-radius.so 0x7f4250b5d000 [0x7f4250b62973]
Feb 21 17:39:57 15[LIB] -> /home/adam/strongswan/src/libcharon/plugins/eap_radius/eap_radius_accounting.c:
630
```

```
if (plain && ike_sa->get_state(ike_sa) == IKE_ESTABLISHED &&
        !incoming && !message->get_request(message))
    {
```

A crash doesn't seem very likely here. ike_sa should definitely be valid, as should message.

But what code base are you using? The line numbers for ike_sa.c in the backtrace don't correspond to the code of the 5.2.2 release (or the current master for that matter). Did you apply any patches?

Perhaps the *eap-radius* plugin is not from the same build as the daemon? This could happen if you built a new version but haven't enabled the plugin. If it was installed with an earlier build it might still get loaded (in particular with the modular config, where plugin snippets in strongswan.d/charon are not removed). If that's the case some of the function pointers on ike_sa and message used by the plugin might not point to the right methods.

#2 - 09.03.2015 03:57 - richard hu

I applied patch but not on ike_sa.c, is this the reason?
we changed some code in eap-radius.
our code is based on 5.2.2 and the build process is standard and configure plugin list is stable every time. and every time server implement is fresh new build and fresh deb install.

#3 - 09.03.2015 11:28 - Tobias Brunner

> I applied patch but not on ike_sa.c, is this the reason?
> we changed some code in eap-radius.

The crash seems to happen in that plugin. So without seeing your changes we can't rule them out as the reason.

#4 - 11.03.2015 03:38 - richard hu

- File eap_radius_diff.txt added

Tobias, attach is diff for my changes on eap_radius plugin.
the changes is to let login user pass authentication when radius connect timeout.
please ignore the logs in the diff, it will gone in prod. and you can also ignore the version is 5.2.1 since these changes do not care 5.2.1 or 5.2.2.

#5 - 11.03.2015 11:17 - Tobias Brunner

> the changes is to let login user pass authentication when radius connect timeout.

Sorry, but that's just plain wrong! With this anybody gains access to your VPN service if your RADIUS server is under heavy load (load that may even be produced by an attacker).

The patch doesn't really explain the crash though. It happens before the authentication via RADIUS even started, so your patch should not have an influence on that (is this the only thing you patched in the whole code base?).

The stacktrace still looks odd to me, for instance, from the process_message() call (ike_sa.c:1362) there is a direct jump to a call to generate_message() (task_manager_v2.c:813). At least two frames are missing there. And I still don't see how there could be a crash on eap_radius_accounting.c:630, both the message and the ike_sa objects were accessed successfully shortly before that. You should make sure that the timestamps of the installed plugins, libraries and executables match, i.e. that all files are from the same build (and that there are no duplicate files from old builds somewhere on your system that might get used inadvertently).

#6 - 02.04.2015 10:36 - Tobias Brunner

- Has duplicate Issue #918: ikev2 crash added

#7 - 07.07.2015 17:22 - Tobias Brunner

- Tracker changed from Issue to Bug

- Subject changed from strongswan server core! to strongswan server core! during IKE_SA rekeying

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

- Resolution set to Fixed

This actually looks like an issue I recently fixed (see last two commits in the *ike-rekey-context* branch), where the IKE_SA on bus_t is set to NULL and subsequent events are therefore called without IKE_SA object.

#8 - 27.07.2015 14:45 - Tobias Brunner

- Status changed from Feedback to Closed

#9 - 30.05.2017 14:05 - Tobias Brunner

- Has duplicate Issue #2345: Crash in ha_ike hook_message added

Files

eap_radius_diff.txt	705 Bytes	11.03.2015	richard hu