strongSwan - Bug #338

Memory of charon keep rising

16.05.2013 11:55 - alma clinton

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.0		
Affected version:	5.0.3	**Resolution:**	Fixed

Description

Hi,
I just upgrade the strongswan from 4.6.4 to 5.0.3. But i still have the problem liked i descripted in issue #306. Last time Martin told me such problem had modified like following:

```
Clean up IKE_SA state if IKE_SA_INIT request does not have message ID 0
author    Martin Willi <martin@revosec.ch>

    Mon, 11 Mar 2013 10:30:47 +0000 (11:30 +0100)
committer    Martin Willi <martin@revosec.ch>

    Mon, 11 Mar 2013 10:30:47 +0000 (11:30 +0100)
src/libcharon/sa/ikev2/task_manager_v2.c
    patch | blob | history

diff --git a/src/libcharon/sa/ikev2/task_manager_v2.c b/src/libcharon/sa/ikev2/task_manager_v2.c
index 29d8d83..a53c06b 100644 (file)

--- a/src/libcharon/sa/ikev2/task_manager_v2.c
+++ b/src/libcharon/sa/ikev2/task_manager_v2.c
@@ -1175,6 +1175,10 @@ METHOD(task_manager_t, process_message, status_t,
         {
             DBG1(DBG_IKE, "received message ID %d, expected %d. Ignored",
                  mid, this->responding.mid);
+            if (msg->get_exchange_type(msg) == IKE_SA_INIT)
+            {   /* clean up IKE_SA state if IKE_SA_INIT has invalid msg ID */
+                return DESTROY_ME;
+            }
         }
```

I had make sure that strongswan 5.0.3 have such code, but when I establish 1000 ipsec tunnels per second last 30s then establish 2 ipsec tunnels per second last 10 minutes with an instrument. But about 4 minutes later, the instrument send out the IKE INIT packet with nonzero message ID, then the memory of charon keep rising until charon was restarted.The memory of charon is as following:

```
 PID USER      STATUS   RSS  PPID %CPU %MEM COMMAND
 2404 root      S       788M 2258  58.1  89.1  charon
```

Any can this problem be resolved ?

Related issues:

Related to Issue #306: The memory of charon process abnormal	**Closed**	**11.03.2013**

History

#1 - 16.05.2013 12:13 - Tobias Brunner

- Description updated

- Priority changed from High to Normal

- Affected version changed from 5.0.4 to 5.0.3

#2 - 16.05.2013 12:13 - Tobias Brunner

- Description updated

#3 - 21.05.2013 14:11 - Tobias Brunner

- Status changed from New to Feedback

> but when I establish 1000 ipsec tunnels per second last 30s then establish 2 ipsec tunnels per second last 10 minutes with an instrument.

Do these SAs get terminated again or do you keep them established? Keep in mind that each established SA requires some resident memory. So if you establish 1000 * 30 + 10 * 60 * 2 = 31'200 IKE SAs don't be surprised if they require hundreds of megabytes of memory.

> But about 4 minutes later, the instrument send out the IKE INIT packet with nonzero message ID, then the memory of charon keep rising until charon was restarted.

You mean the memory rises even if you don't establish regular IKE SAs in the background? You just send invalid IKE_SA_INIT messages? Unfortunately, you haven't answered Martin's questions from his mail in response to #306.

Could you send us the tool/script you use to test this? So we could try to reproduce this situation and investigate further.

#4 - 23.05.2013 10:43 - Andreas Steffen

- Assignee set to Tobias Brunner

#5 - 20.06.2013 11:00 - alma clinton

I am so sorry did not reply in time.
In my experiment, SAs get terminated again.And the avariable memory of linux is 2G.

>> You mean the memory rises even if you don't establish regular IKE SAs in the >>background? You just send invalid IKE_SA_INIT messages?

Yes,even if it don't establish regular IKE SAs in the background and it just send invalid IKE_SA_INIT messages the memory of charon keep rising.

>> Could you send us the tool/script you use to test this?

I do experiments based on Spirent TestCenter Layer 4-7 Application 4.20,base model :SPT-3100,Model/SN:CEE-3100B R 11141003.

>> You'll have to provide some more details what is happening to analyze
>> this issue. Are these IKE_SA_INITs for the same IKE_SA?

yes,these IKE_SA_INITs for the same IKE_SA.

>> Using the same SPI?

Did you mean the ike SPI?It use the same IKE cookies we found from the pcaket.

>> What does charon log for the first and the second IKE_SA_INIT message?

the normol message is as following:

```
Jun 29 09:59:28 11[NET] <1> received packet: from 10.0.4.0^{500} to 10.2.0.5^{500}
Jun 29 09:59:28 11[ENC] <1> parsed IKE_SA_INIT request 0 [ SA KE No V ]
Jun 29 09:59:28 11[ENC] <1> received unknown vendor id:
53:70:69:72:65:6e:74:20:43:6f:6d:6d:75:6e:69:63:61:74:69:6f:6e:73:20:49:6e:63:20:33:37:2e:34:31:34:35:2c:2d:31:32:32:2e:30:31:37:34
Jun 29 09:59:28 11[IKE] <1> 10.0.4.0 is initiating an IKE_SA
Jun 29 09:59:28 11[ENC] <1> generating IKE_SA_INIT response 0 [ SA KE No N(MULT_AUTH) ]
Jun 29 09:59:28 11[NET] <1> sending packet: from 10.2.0.5^{500} to 10.0.4.0^{500}
Jun 29 09:59:28 12[NET] <1> received packet: from 10.0.4.0^{500} to 10.2.0.5^{500}
Jun 29 09:59:28 12[ENC] <1> parsed IKE_AUTH request 1 [ IDi AUTH SA TSi TSr N(MULT_AUTH) ]
Jun 29 09:59:28 12[CFG] <1> looking for peer configs matching 10.2.0.5[%any]...10.0.4.0[a1]
Jun 29 09:59:28 12[CFG] <au-gw1|1> selected peer config 'au-gw1'
Jun 29 09:59:28 12[IKE] <au-gw1|1> authentication of 'a1' with pre-shared key successful
Jun 29 09:59:28 12[IKE] <au-gw1|1> authentication of 'comba.com.cn' (myself) with pre-shared key
Jun 29 09:59:28 12[IKE] <au-gw1|1> IKE_SA au-gw1[1] established between 10.2.0.5[comba.com.cn]...10.0.4.0[a1]
Jun 29 09:59:28 12[IKE] <au-gw1|1> CHILD_SA au-gw1{1} established with SPIs c66c6349_i 30f5fc8a_o and TS 10.7.0.1..10.7.100.100 ===
10.0.4.0/32
Jun 29 09:59:28 12[ENC] <au-gw1|1> generating IKE_AUTH response 1 [ IDr AUTH SA TSi TSr ]
```

the abnormol message is as following:

```
Apr  1 08:41:53 (none) daemon.info charon: 271[NET] received packet: from 10.0.13.223[500] to 10.2.0.5[500]
Apr  1 08:41:53 (none) daemon.info charon: 271[ENC] parsed IKE_SA_INIT request 2 [ SA KE No V ]
Apr  1 08:41:53 (none) daemon.info charon: 271[IKE] received message ID 2, expected 0. Ignored
```

thank you very much for your attention!

#6 - 25.07.2013 13:51 - Tobias Brunner

- File 0001-ikev2-Only-schedule-half-open-timeout-delete-job-aft.patch added

- Tracker changed from Issue to Bug

- Category set to charon

I tried to reproduce this and I think the increase in memory you see is caused by the jobs that are scheduled to delete half-open IKE_SAs, which are needed if the client only sends a valid *IKE_SA_INIT* but never sends an *IKE_AUTH* request. Such jobs were also scheduled if the IKE_SA was deleted immediately due to an invalid *IKE_SA_INIT* message.

Please try the attached patch, which schedules the job only if the initial message was handled successfully.

#7 - 29.07.2013 11:29 - Tobias Brunner

- Status changed from Feedback to Closed

- Target version set to 5.1.0

- Resolution set to Fixed

Files

0001-ikev2-Only-schedule-half-open-timeout-delete-job-aft.patch	2.43 KB	25.07.2013	Tobias Brunner