strongSwan - Bug #3060

IKEv1: initial/non-rekey QM collision results in uneven updown events

15.05.2019 09:28 - Daniel Gollub

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.8.1		
Affected version:	dr|rc|master	**Resolution:**	Fixed

Description

IKEv1 specific. IKEv2 is not affected by this.

#2902 resolved uneven updown/close events by detecting redundant Child SAs in the quick_delete task.

The detection and suppression of updown events is not done in the quick_mode task and might result in uneven updown events, by not suppressing child_updown UP event in case of a redundant SA.

Logs indicating the uneven updown event, caused by a QM collision, of Child SA which have not yet been rekeyed:

(rc/master: 802da663c200f)

```
[...]
14:12:28 dut charon[29367]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (87 bytes)
14:12:28 dut charon[29367]: 09[ENC] parsed ID_PROT request 0 [ SA ]
14:12:28 dut charon[29367]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
14:12:28 dut charon[29367]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
14:12:28 dut charon[29367]: 09[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
14:12:28 dut charon[29367]: 09[ENC] generating ID_PROT response 0 [ SA V V ]
14:12:28 dut charon[29367]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (120 bytes)
14:12:28 dut charon[29367]: 10[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (236 bytes)
14:12:28 dut charon[29367]: 10[ENC] parsed ID_PROT request 0 [ KE No ]
14:12:28 dut charon[29367]: 10[ENC] generating ID_PROT response 0 [ KE No ]
14:12:28 dut charon[29367]: 10[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (260 bytes)
14:12:28 dut charon[29367]: 11[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)
14:12:28 dut charon[29367]: 11[ENC] parsed ID_PROT request 0 [ ID HASH ]
14:12:28 dut charon[29367]: 11[CFG] looking for pre-shared key peer configs matching 192.168.252.131...192.168.252.4[192.168.252.4]
14:12:28 dut charon[29367]: 11[CFG] selected peer config "collision-test"
14:12:28 dut charon[29367]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.131]...192.168.252.4[192.168.252.4]
14:12:28 dut charon[29367]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.131]...192.168.252.4[192.168.252.4]
14:12:28 dut charon[29367]: 11[IKE] scheduling reauthentication in 28800s
14:12:28 dut charon[29367]: 11[IKE] maximum IKE_SA lifetime 28800s
14:12:28 dut charon[29367]: 11[ENC] generating ID_PROT response 0 [ ID HASH ]
14:12:28 dut charon[29367]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
14:12:31 dut charon[29367]: 13[CFG] received stroke: initiate 'collision-test'
14:12:31 dut charon[29367]: 15[ENC] generating QUICK_MODE request 949434017 [ HASH SA No KE ID ID ]
14:12:31 dut charon[29367]: 15[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
14:12:34 dut charon[29367]: 16[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes)
```

```
14:12:34 dut charon[29367]: 16[ENC] parsed QUICK_MODE request 3588192074 [ HASH SA No KE ID ID ]
14:12:34 dut charon[29367]: 16[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_E
XT_SEQ
14:12:34 dut charon[29367]: 16[ENC] generating QUICK_MODE response 3588192074 [ HASH SA No KE ID I
D ]
14:12:34 dut charon[29367]: 16[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500
] (380 bytes)
14:12:34 dut charon[29367]: 06[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[50
0] (364 bytes)
14:12:34 dut charon[29367]: 06[ENC] parsed QUICK_MODE response 949434017 [ HASH SA No KE ID ID ]
14:12:34 dut charon[29367]: 06[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_E
XT_SEQ
14:12:34 dut charon[29367]: 06[IKE] CHILD_SA collision-test{1} established with SPIs cf9c62a3_i 6e
0f9ad4_o and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:34 dut charon[29367]: 06[IKE] CHILD_SA collision-test{1} established with SPIs cf9c62a3_i 6e
0f9ad4_o and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_VERSION=1.1
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_CONNECTION=collision-test
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_MY_PORT=0
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PEER_PROTOCOL=0
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PEER=192.168.252.4
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_VERB=up-client
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PEER_PORT=0
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_ME=192.168.252.131
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PEER_ID=192.168.252.4
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_REQID=1
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_MY_ID=192.168.252.131
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_MY_PROTOCOL=0
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PROTO=esp
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_UNIQUEID=1
14:12:34 dut charon[29367]: 06[CHD] updown: PLUTO_INTERFACE=dp0s2
14:12:34 dut charon[29367]: 06[ENC] generating QUICK_MODE request 949434017 [ HASH ]
14:12:34 dut charon[29367]: 06[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500
] (60 bytes)
14:12:34 dut charon[29367]: 05[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[50
0] (60 bytes)
14:12:34 dut charon[29367]: 05[ENC] parsed QUICK_MODE request 3588192074 [ HASH ]
14:12:34 dut charon[29367]: 05[IKE] CHILD_SA collision-test{2} established with SPIs cd178057_i 23
913f83_o and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:34 dut charon[29367]: 05[IKE] CHILD_SA collision-test{2} established with SPIs cd178057_i 23
913f83_o and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_VERSION=1.1
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_CONNECTION=collision-test
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_MY_PORT=0
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PEER_PROTOCOL=0
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PEER=192.168.252.4
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_VERB=up-client
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PEER_PORT=0
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_ME=192.168.252.131
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PEER_ID=192.168.252.4
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_REQID=1
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_MY_ID=192.168.252.131
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_MY_PROTOCOL=0
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PROTO=esp
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_UNIQUEID=1
14:12:34 dut charon[29367]: 05[CHD] updown: PLUTO_INTERFACE=dp0s2
14:12:47 dut charon[29367]: 10[CFG] vici terminate IKE_SA 'collision-test'
14:12:47 dut charon[29367]: 12[IKE] detected redundant CHILD_SA collision-test{1}
14:12:47 dut charon[29367]: 12[IKE] closing CHILD_SA collision-test{1} with SPIs cf9c62a3_i (0 byt
es) 6e0f9ad4_o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:47 dut charon[29367]: 12[IKE] closing CHILD_SA collision-test{1} with SPIs cf9c62a3_i (0 byt
es) 6e0f9ad4_o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:47 dut charon[29367]: 12[IKE] sending DELETE for ESP CHILD_SA with SPI cf9c62a3
```

```
14:12:47 dut charon[29367]: 12[ENC] generating INFORMATIONAL_V1 request 2397896470 [ HASH D ]
14:12:47 dut charon[29367]: 12[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500
] (76 bytes)
14:12:47 dut charon[29367]: 12[IKE] closing CHILD_SA collision-test{2} with SPIs cd178057_i (0 byt
es) 23913f83_o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:47 dut charon[29367]: 12[IKE] closing CHILD_SA collision-test{2} with SPIs cd178057_i (0 byt
es) 23913f83_o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
14:12:47 dut charon[29367]: 12[CHD] updown: PLUTO_VERSION=1.1
14:12:47 dut charon[29367]: 12[CHD] updown: PLUTO_CONNECTION=collision-test
14:12:47 dut charon[29367]: 12[CHD] updown: PLUTO_MY_PORT=0
14:12:47 dut charon[29367]: 12[CHD] updown: PLUTO_PEER_PROTOCOL=0
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_PEER=192.168.252.4
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_VERB=down-client
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_PEER_PORT=0
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_ME=192.168.252.131
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_PEER_ID=192.168.252.4
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_REQID=1
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_MY_ID=192.168.252.131
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_MY_PROTOCOL=0
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_PROTO=esp
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_UNIQUEID=1
14:12:48 dut charon[29367]: 12[CHD] updown: PLUTO_INTERFACE=dp0s2
14:12:48 dut charon[29367]: 12[IKE] sending DELETE for ESP CHILD_SA with SPI cd178057
14:12:48 dut charon[29367]: 12[ENC] generating INFORMATIONAL_V1 request 792874482 [ HASH D ]
14:12:48 dut charon[29367]: 12[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500
] (76 bytes)
14:12:48 dut charon[29367]: 12[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.
168.252.131]...192.168.252.4[192.168.252.4]
14:12:48 dut charon[29367]: 12[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.
168.252.131]...192.168.252.4[192.168.252.4]
14:12:48 dut charon[29367]: 12[IKE] sending DELETE for IKE_SA collision-test[1]
14:12:48 dut charon[29367]: 12[ENC] generating INFORMATIONAL_V1 request 1192740568 [ HASH D ]
14:12:48 dut charon[29367]: 12[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500
] (92 bytes)
```

Associated revisions

Revision 71141cc8 - 22.05.2019 18:28 - Tobias Brunner

ikev1: Do a rekey check before installing CHILD_SAs as responder

If CHILD_SAs are created while waiting for the third QM message we'd not notice the redundancy and updown events would be triggered unevenly. This is consistent with the behavior on the initiator, which already does this check right before installation. Moving the existing check is not possible due to the narrow hook and moving the installation changes which peer installs the SAs first and could have other side-effects (e.g. in error or conflict cases). Still, this might result in CHILD_SA state discrepancies between the two peers.

Fixes #3060.

History

#1 - 15.05.2019 09:34 - Daniel Gollub

Potential fix:
https://github.com/strongswan/strongswan/pull/139

Logs with patch applied:

```
09:32:28 dut charon[4469]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (87 bytes)
09:32:28 dut charon[4469]: 09[ENC] parsed ID_PROT request 0 [ SA ]
09:32:28 dut charon[4469]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
09:32:28 dut charon[4469]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
09:32:28 dut charon[4469]: 09[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
09:32:28 dut charon[4469]: 09[ENC] generating ID_PROT response 0 [ SA V V ]
09:32:28 dut charon[4469]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (120 bytes)
09:32:28 dut charon[4469]: 10[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (236 bytes
```

```
)
09:32:28 dut charon[4469]: 10[ENC] parsed ID_PROT request 0 [ KE No ]
09:32:28 dut charon[4469]: 10[ENC] generating ID_PROT response 0 [ KE No ]
09:32:28 dut charon[4469]: 10[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (260 bytes)
09:32:28 dut charon[4469]: 11[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)
09:32:28 dut charon[4469]: 11[ENC] parsed ID_PROT request 0 [ ID HASH ]
09:32:28 dut charon[4469]: 11[CFG] looking for pre-shared key peer configs matching 192.168.252.131...192.168.
252.4[192.168.252.4]
09:32:28 dut charon[4469]: 11[CFG] selected peer config "collision-test"
09:32:28 dut charon[4469]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
09:32:28 dut charon[4469]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
09:32:28 dut charon[4469]: 11[IKE] scheduling reauthentication in 28800s
09:32:28 dut charon[4469]: 11[IKE] maximum IKE_SA lifetime 28800s
09:32:28 dut charon[4469]: 11[ENC] generating ID_PROT response 0 [ ID HASH ]
09:32:28 dut charon[4469]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
09:32:51 dut charon[4469]: 06[CFG] vici initiate CHILD_SA 'collision-test'
09:32:51 dut charon[4469]: 05[ENC] generating QUICK_MODE request 1277059208 [ HASH SA No KE ID ID ]
09:32:51 dut charon[4469]: 05[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
09:32:53 dut charon[4469]: 10[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
09:32:53 dut charon[4469]: 10[ENC] parsed QUICK_MODE request 2650360249 [ HASH SA No KE ID ID ]
09:32:53 dut charon[4469]: 10[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
09:32:53 dut charon[4469]: 10[ENC] generating QUICK_MODE response 2650360249 [ HASH SA No KE ID ID ]
09:32:53 dut charon[4469]: 10[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
09:32:53 dut charon[4469]: 12[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
09:32:53 dut charon[4469]: 12[ENC] parsed QUICK_MODE response 1277059208 [ HASH SA No KE ID ID ]
09:32:53 dut charon[4469]: 12[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
09:32:53 dut charon[4469]: 12[IKE] CHILD_SA collision-test{1} established with SPIs c98faab0_i d3b0cd65_o and
TS 10.10.3.0/24 === 10.10.1.0/24
09:32:53 dut charon[4469]: 12[IKE] CHILD_SA collision-test{1} established with SPIs c98faab0_i d3b0cd65_o and
TS 10.10.3.0/24 === 10.10.1.0/24
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_VERSION=1.1
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_CONNECTION=collision-test
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_MY_PORT=0
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PEER_PROTOCOL=0
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PEER=192.168.252.4
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_VERB=up-client
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PEER_PORT=0
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_ME=192.168.252.131
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PEER_ID=192.168.252.4
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_REQID=1
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_MY_ID=192.168.252.131
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_MY_PROTOCOL=0
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PROTO=esp
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_UNIQUEID=1
09:32:53 dut charon[4469]: 12[CHD] updown: PLUTO_INTERFACE=dp0s2
09:32:53 dut charon[4469]: 12[ENC] generating QUICK_MODE request 1277059208 [ HASH ]
09:32:53 dut charon[4469]: 12[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (60 bytes)
09:32:53 dut charon[4469]: 15[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (60 bytes)
09:32:53 dut charon[4469]: 15[ENC] parsed QUICK_MODE request 2650360249 [ HASH ]
09:32:53 dut charon[4469]: 15[IKE] CHILD_SA collision-test{2} established with SPIs c91263a1_i 3cb5267d_o and
TS 10.10.3.0/24 === 10.10.1.0/24
09:32:53 dut charon[4469]: 15[IKE] CHILD_SA collision-test{2} established with SPIs c91263a1_i 3cb5267d_o and
TS 10.10.3.0/24 === 10.10.1.0/24
09:32:53 dut charon[4469]: 15[IKE] detected redundant CHILD_SA collision-test{2}
09:33:00 dut charon[4469]: 05[CFG] vici terminate IKE_SA 'collision-test'
09:33:00 dut charon[4469]: 13[IKE] detected redundant CHILD_SA collision-test{1}
09:33:00 dut charon[4469]: 13[IKE] closing CHILD_SA collision-test{1} with SPIs c98faab0_i (0 bytes) d3b0cd65_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
09:33:00 dut charon[4469]: 13[IKE] closing CHILD_SA collision-test{1} with SPIs c98faab0_i (0 bytes) d3b0cd65_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
09:33:00 dut charon[4469]: 13[IKE] sending DELETE for ESP CHILD_SA with SPI c98faab0
09:33:00 dut charon[4469]: 13[ENC] generating INFORMATIONAL_V1 request 1376071932 [ HASH D ]
09:33:00 dut charon[4469]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
09:33:00 dut charon[4469]: 13[IKE] closing CHILD_SA collision-test{2} with SPIs c91263a1_i (0 bytes) 3cb5267d_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
09:33:00 dut charon[4469]: 13[IKE] closing CHILD_SA collision-test{2} with SPIs c91263a1_i (0 bytes) 3cb5267d_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_VERSION=1.1
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_CONNECTION=collision-test
```

```
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_MY_PORT=0
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PEER_PROTOCOL=0
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PEER=192.168.252.4
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_VERB=down-client
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PEER_PORT=0
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_ME=192.168.252.131
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PEER_ID=192.168.252.4
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_REQID=1
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_MY_ID=192.168.252.131
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_MY_PROTOCOL=0
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PROTO=esp
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_UNIQUEID=1
09:33:00 dut charon[4469]: 13[CHD] updown: PLUTO_INTERFACE=dp0s2
09:33:00 dut charon[4469]: 13[IKE] sending DELETE for ESP CHILD_SA with SPI c91263a1
09:33:00 dut charon[4469]: 13[ENC] generating INFORMATIONAL_V1 request 2174283093 [ HASH D ]
09:33:00 dut charon[4469]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
09:33:00 dut charon[4469]: 13[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
09:33:00 dut charon[4469]: 13[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
09:33:00 dut charon[4469]: 13[IKE] sending DELETE for IKE_SA collision-test[1]
09:33:00 dut charon[4469]: 13[ENC] generating INFORMATIONAL_V1 request 4142037756 [ HASH D ]
09:33:00 dut charon[4469]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (92 bytes)
```

#2 - 16.05.2019 10:57 - Tobias Brunner

- Status changed from New to Feedback

Looks like a race condition. If the CHILD_SA installed as responder was established first (i.e. before the response to the QM request is received), I think this would be detected are rekeying.

That's because, as initiator, the check for existing CHILD_SAs happens after processing the second QM message and right before install() is called (i.e. the additional check you added would be redundant). However, as responder, that rekey check happens when the initial QM request is processed, the installation, on the other hand (including the check you added), is delayed until the third QM message is received.

That the check happens earlier is due to the call to the narrow() hook, which expects a CHILD_SA object. So that has to be created then, which requires retrieving information from any existing CHILD_SA. So even with your patch the behavior might not be entirely consistent (it would fix the child-updown issue, but child-rekey might or might not be called and the state of the existing SA might or might not get changed depending on the timing of the exchanged packets).

I guess we could get a more consistent behavior either by adding another rekey check before the installation and create a new CHILD_SA object if necessary (i.e. if a redundant SA is now found). Or by moving the installation right after the creation of the CHILD_SA object (making the responder use the CHILD_SA earlier than the initiator during rekeyings, the reverse is currently true - we could even install the inbound SA first and the outbound SA later when the third QM message is received, but that would require a lot more modifications and change the behavior even more). The former is quite simple to implement and has probably less side-effects overall. So I pushed that change to the *3060-ikev1-child-rekey-check* branch.

#3 - 16.05.2019 12:09 - Daniel Gollub

> Looks like a race condition. If the CHILD_SA installed as responder was established first (i.e. before the response to the QM request is received), I think this would be detected are rekeying.

That's also my understanding. That seems to be the case in the issue reported in #2902 and for that reason I haven't focused on the child_updown UP event case and just focused on suppressing the child_updown DOWN (and close_action) to maintain an even number.

> So even with your patch the behavior might not be entirely consistent (it would fix the child-updown issue, but child-rekey might or might not be called and the state of the existing SA might or might not get changed depending on the timing of the exchanged packets).

Thanks for clarifying this. I hesitated to mark a redundant Child SA right on it's creation as rekeyed, because I wasn't sure about potential side-effects. IIUC for the IKEv1 CHILD_SA handling having a CHILD_SA state set to REKEYED probably is just going to influence: updown and close action triggering behavior.

Another "special" case would be if charon.delete_rekeyed=yes is set. When marking the redundant CHILD_SA as rekeyed, shouldn't the install() call later also wipe the CHILD_SA which just got marked as "rekeyed"? I did gave this a quick try, that seems to be not the case. (But I wouldn't mind either, I guess redundant CHILD_SAs are rather rare. So not sure if there is so much benefit if charon.delete_rekeyed=yes really has to wipe everything and redundant CHILD_SA might be considered as exception?)

I gave e7f8f7da3b1de677a70 a quick try and verified it solves the uneven child-updown for this particular race condition:

(charon.delete_rekeyed=no)

```
11:13:51 dut charon[8709]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (87 bytes)
11:13:51 dut charon[8709]: 09[ENC] parsed ID_PROT request 0 [ SA ]
11:13:51 dut charon[8709]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
11:13:51 dut charon[8709]: 09[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
11:13:51 dut charon[8709]: 09[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
11:13:51 dut charon[8709]: 09[ENC] generating ID_PROT response 0 [ SA V V ]
11:13:51 dut charon[8709]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (120 bytes)
11:13:51 dut charon[8709]: 10[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (236 bytes
)
11:13:51 dut charon[8709]: 10[ENC] parsed ID_PROT request 0 [ KE No ]
11:13:51 dut charon[8709]: 10[ENC] generating ID_PROT response 0 [ KE No ]
11:13:51 dut charon[8709]: 10[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (260 bytes)
11:13:51 dut charon[8709]: 11[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)
11:13:51 dut charon[8709]: 11[ENC] parsed ID_PROT request 0 [ ID HASH ]
11:13:51 dut charon[8709]: 11[CFG] looking for pre-shared key peer configs matching 192.168.252.131...192.168.
252.4[192.168.252.4]
11:13:51 dut charon[8709]: 11[CFG] selected peer config "collision-test"
11:13:51 dut charon[8709]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
11:13:51 dut charon[8709]: 11[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
11:13:51 dut charon[8709]: 11[IKE] scheduling reauthentication in 28800s
11:13:51 dut charon[8709]: 11[IKE] maximum IKE_SA lifetime 28800s
11:13:51 dut charon[8709]: 11[ENC] generating ID_PROT response 0 [ ID HASH ]
11:13:51 dut charon[8709]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:13:53 dut charon[8709]: 14[CFG] vici initiate CHILD_SA 'collision-test'
11:13:53 dut charon[8709]: 15[ENC] generating QUICK_MODE request 4225651501 [ HASH SA No KE ID ID ]
11:13:53 dut charon[8709]: 15[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)

11:13:55 dut charon[8709]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
11:13:55 dut charon[8709]: 09[ENC] parsed QUICK_MODE request 2511526207 [ HASH SA No KE ID ID ]
11:13:55 dut charon[8709]: 09[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
11:13:55 dut charon[8709]: 09[ENC] generating QUICK_MODE response 2511526207 [ HASH SA No KE ID ID ]
11:13:55 dut charon[8709]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
11:13:55 dut charon[8709]: 16[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
11:13:55 dut charon[8709]: 16[ENC] parsed QUICK_MODE response 4225651501 [ HASH SA No KE ID ID ]
11:13:55 dut charon[8709]: 16[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
11:13:55 dut charon[8709]: 16[IKE] CHILD_SA collision-test{1} established with SPIs ce353c0a_i 403b3dbe_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:13:55 dut charon[8709]: 16[IKE] CHILD_SA collision-test{1} established with SPIs ce353c0a_i 403b3dbe_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_VERSION=1.1
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_CONNECTION=collision-test
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_MY_PORT=0
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PEER_PROTOCOL=0
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PEER=192.168.252.4
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_VERB=up-client
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PEER_PORT=0
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_ME=192.168.252.131
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PEER_ID=192.168.252.4
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_REQID=1
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_MY_ID=192.168.252.131
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_MY_PROTOCOL=0
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PROTO=esp
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_UNIQUEID=1
11:13:55 dut charon[8709]: 16[CHD] updown: PLUTO_INTERFACE=dp0s2
11:13:55 dut charon[8709]: 16[ENC] generating QUICK_MODE request 4225651501 [ HASH ]
11:13:55 dut charon[8709]: 16[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (60 bytes)
11:13:55 dut charon[8709]: 10[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (60 bytes)
11:13:55 dut charon[8709]: 10[ENC] parsed QUICK_MODE request 2511526207 [ HASH ]
11:13:55 dut charon[8709]: 10[IKE] detected rekeying of CHILD_SA collision-test{1}
11:13:55 dut charon[8709]: 10[IKE] CHILD_SA collision-test{3} established with SPIs c0e3eec0_i e7732c30_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:13:55 dut charon[8709]: 10[IKE] CHILD_SA collision-test{3} established with SPIs c0e3eec0_i e7732c30_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:14:02 dut charon[8709]: 12[CFG] vici terminate IKE_SA 'collision-test'
11:14:02 dut charon[8709]: 13[IKE] closing CHILD_SA collision-test{1} with SPIs ce353c0a_i (0 bytes) 403b3dbe_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:14:02 dut charon[8709]: 13[IKE] closing CHILD_SA collision-test{1} with SPIs ce353c0a_i (0 bytes) 403b3dbe_
```

```
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:14:02 dut charon[8709]: 13[IKE] sending DELETE for ESP CHILD_SA with SPI ce353c0a
11:14:02 dut charon[8709]: 13[ENC] generating INFORMATIONAL_V1 request 2571211748 [ HASH D ]
11:14:02 dut charon[8709]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:14:02 dut charon[8709]: 13[IKE] closing CHILD_SA collision-test{3} with SPIs c0e3eec0_i (0 bytes) e7732c30_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:14:02 dut charon[8709]: 13[IKE] closing CHILD_SA collision-test{3} with SPIs c0e3eec0_i (0 bytes) e7732c30_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_VERSION=1.1
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_CONNECTION=collision-test
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_MY_PORT=0
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PEER_PROTOCOL=0
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PEER=192.168.252.4
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_VERB=down-client
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PEER_PORT=0
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_ME=192.168.252.131
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PEER_ID=192.168.252.4
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_REQID=1
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_MY_ID=192.168.252.131
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_MY_PROTOCOL=0
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PROTO=esp
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_UNIQUEID=1
11:14:02 dut charon[8709]: 13[CHD] updown: PLUTO_INTERFACE=dp0s2
11:14:02 dut charon[8709]: 13[IKE] sending DELETE for ESP CHILD_SA with SPI c0e3eec0
11:14:02 dut charon[8709]: 13[ENC] generating INFORMATIONAL_V1 request 2047932351 [ HASH D ]
11:14:02 dut charon[8709]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:14:02 dut charon[8709]: 13[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
11:14:02 dut charon[8709]: 13[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
11:14:02 dut charon[8709]: 13[IKE] sending DELETE for IKE_SA collision-test[1]
11:14:02 dut charon[8709]: 13[ENC] generating INFORMATIONAL_V1 request 2231111382 [ HASH D ]
11:14:02 dut charon[8709]: 13[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (92 bytes)
```

With charon.delete_rekeyed=yes

```
12:10:31 dut charon[9412]: 07[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (87 bytes)

12:10:31 dut charon[9412]: 07[ENC] parsed ID_PROT request 0 [ SA ]
12:10:31 dut charon[9412]: 07[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
12:10:31 dut charon[9412]: 07[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
12:10:31 dut charon[9412]: 07[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
12:10:31 dut charon[9412]: 07[ENC] generating ID_PROT response 0 [ SA V V ]
12:10:31 dut charon[9412]: 07[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (120 bytes)

12:10:31 dut charon[9412]: 08[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (236 bytes
)
12:10:31 dut charon[9412]: 08[ENC] parsed ID_PROT request 0 [ KE No ]
12:10:31 dut charon[9412]: 08[ENC] generating ID_PROT response 0 [ KE No ]
12:10:31 dut charon[9412]: 08[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (260 bytes)

12:10:31 dut charon[9412]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)

12:10:31 dut charon[9412]: 09[ENC] parsed ID_PROT request 0 [ ID HASH ]
12:10:31 dut charon[9412]: 09[CFG] looking for pre-shared key peer configs matching 192.168.252.131...192.168.
252.4[192.168.252.4]
12:10:31 dut charon[9412]: 09[CFG] selected peer config "collision-test"
12:10:31 dut charon[9412]: 09[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
12:10:31 dut charon[9412]: 09[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
12:10:31 dut charon[9412]: 09[IKE] scheduling reauthentication in 28800s
12:10:31 dut charon[9412]: 09[IKE] maximum IKE_SA lifetime 28800s
12:10:31 dut charon[9412]: 09[ENC] generating ID_PROT response 0 [ ID HASH ]
12:10:31 dut charon[9412]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
12:10:33 dut charon[9412]: 12[CFG] vici initiate CHILD_SA 'collision-test'
12:10:33 dut charon[9412]: 14[ENC] generating QUICK_MODE request 3058275592 [ HASH SA No KE ID ID ]
12:10:33 dut charon[9412]: 14[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)

12:10:34 dut charon[9412]: 16[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
12:10:34 dut charon[9412]: 16[ENC] parsed QUICK_MODE request 3442688460 [ HASH SA No KE ID ID ]
12:10:34 dut charon[9412]: 16[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
```

```
12:10:34 dut charon[9412]: 16[ENC] generating QUICK_MODE response 3442688460 [ HASH SA No KE ID ID ]
12:10:34 dut charon[9412]: 16[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)

12:10:34 dut charon[9412]: 05[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
12:10:34 dut charon[9412]: 05[ENC] parsed QUICK_MODE response 3058275592 [ HASH SA No KE ID ID ]
12:10:34 dut charon[9412]: 05[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
12:10:34 dut charon[9412]: 05[IKE] CHILD_SA collision-test{1} established with SPIs c8df3382_i 909e2c1a_o and
TS 10.10.3.0/24 === 10.10.1.0/24
12:10:34 dut charon[9412]: 05[IKE] CHILD_SA collision-test{1} established with SPIs c8df3382_i 909e2c1a_o and
TS 10.10.3.0/24 === 10.10.1.0/24
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_VERSION=1.1
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_CONNECTION=collision-test
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_MY_PORT=0
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PEER_PROTOCOL=0
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PEER=192.168.252.4
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_VERB=up-client
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PEER_PORT=0
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_ME=192.168.252.131
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PEER_ID=192.168.252.4
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_REQID=1
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_MY_ID=192.168.252.131
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_MY_PROTOCOL=0
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PROTO=esp
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_UNIQUEID=1
12:10:34 dut charon[9412]: 05[CHD] updown: PLUTO_INTERFACE=dp0s2
12:10:34 dut charon[9412]: 05[ENC] generating QUICK_MODE request 3058275592 [ HASH ]
12:10:34 dut charon[9412]: 05[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (60 bytes)
12:10:34 dut charon[9412]: 11[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (60 bytes)

12:10:34 dut charon[9412]: 11[ENC] parsed QUICK_MODE request 3442688460 [ HASH ]
12:10:34 dut charon[9412]: 11[IKE] detected rekeying of CHILD_SA collision-test{1}
12:10:34 dut charon[9412]: 11[IKE] CHILD_SA collision-test{3} established with SPIs c3868c00_i 2041bab8_o and
TS 10.10.3.0/24 === 10.10.1.0/24
12:10:34 dut charon[9412]: 11[IKE] CHILD_SA collision-test{3} established with SPIs c3868c00_i 2041bab8_o and
TS 10.10.3.0/24 === 10.10.1.0/24
12:10:37 dut charon[9412]: 10[CFG] vici terminate IKE_SA 'collision-test'
12:10:37 dut charon[9412]: 15[IKE] closing CHILD_SA collision-test{1} with SPIs c8df3382_i (0 bytes) 909e2c1a_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
12:10:37 dut charon[9412]: 15[IKE] closing CHILD_SA collision-test{1} with SPIs c8df3382_i (0 bytes) 909e2c1a_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
12:10:37 dut charon[9412]: 15[IKE] sending DELETE for ESP CHILD_SA with SPI c8df3382
12:10:37 dut charon[9412]: 15[ENC] generating INFORMATIONAL_V1 request 2499938949 [ HASH D ]
12:10:37 dut charon[9412]: 15[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
12:10:37 dut charon[9412]: 15[IKE] closing CHILD_SA collision-test{3} with SPIs c3868c00_i (0 bytes) 2041bab8_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
12:10:37 dut charon[9412]: 15[IKE] closing CHILD_SA collision-test{3} with SPIs c3868c00_i (0 bytes) 2041bab8_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_VERSION=1.1
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_CONNECTION=collision-test
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_MY_PORT=0
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PEER_PROTOCOL=0
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PEER=192.168.252.4
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_VERB=down-client
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PEER_PORT=0
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_ME=192.168.252.131
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PEER_ID=192.168.252.4
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_REQID=1
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_MY_ID=192.168.252.131
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_MY_PROTOCOL=0
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PROTO=esp
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_UNIQUEID=1
12:10:38 dut charon[9412]: 15[CHD] updown: PLUTO_INTERFACE=dp0s2
12:10:38 dut charon[9412]: 15[IKE] sending DELETE for ESP CHILD_SA with SPI c3868c00
12:10:38 dut charon[9412]: 15[ENC] generating INFORMATIONAL_V1 request 3613424590 [ HASH D ]
12:10:38 dut charon[9412]: 15[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
12:10:38 dut charon[9412]: 15[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
12:10:38 dut charon[9412]: 15[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
12:10:38 dut charon[9412]: 15[IKE] sending DELETE for IKE_SA collision-test[1]
```

```
12:10:38 dut charon[9412]: 15[ENC] generating INFORMATIONAL_V1 request 1868394369 [ HASH D ]
12:10:38 dut charon[9412]: 15[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (92 bytes)
```

I also verified the scenario from #2902 still maintains an even number of updown events with your patch applied:
(charon.delete_rekeyed=no)

```
11:28:24 dut charon[8866]: 07[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (87 bytes)
11:28:24 dut charon[8866]: 07[ENC] parsed ID_PROT request 0 [ SA ]
11:28:24 dut charon[8866]: 07[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
11:28:24 dut charon[8866]: 07[IKE] 192.168.252.4 is initiating a Main Mode IKE_SA
11:28:24 dut charon[8866]: 07[CFG] selected proposal: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1536
11:28:24 dut charon[8866]: 07[ENC] generating ID_PROT response 0 [ SA V V ]
11:28:24 dut charon[8866]: 07[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (120 bytes)
11:28:24 dut charon[8866]: 08[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (236 bytes
)
11:28:24 dut charon[8866]: 08[ENC] parsed ID_PROT request 0 [ KE No ]
11:28:24 dut charon[8866]: 08[ENC] generating ID_PROT response 0 [ KE No ]
11:28:24 dut charon[8866]: 08[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (260 bytes)
11:28:24 dut charon[8866]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)
11:28:24 dut charon[8866]: 09[ENC] parsed ID_PROT request 0 [ ID HASH ]
11:28:24 dut charon[8866]: 09[CFG] looking for pre-shared key peer configs matching 192.168.252.131...192.168.
252.4[192.168.252.4]
11:28:24 dut charon[8866]: 09[CFG] selected peer config "collision-test"
11:28:24 dut charon[8866]: 09[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
11:28:24 dut charon[8866]: 09[IKE] IKE_SA collision-test[1] established between 192.168.252.131[192.168.252.13
1]...192.168.252.4[192.168.252.4]
11:28:24 dut charon[8866]: 09[IKE] scheduling reauthentication in 28800s
11:28:24 dut charon[8866]: 09[IKE] maximum IKE_SA lifetime 28800s
11:28:24 dut charon[8866]: 09[ENC] generating ID_PROT response 0 [ ID HASH ]
11:28:24 dut charon[8866]: 09[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:28:24 dut charon[8866]: 11[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
11:28:24 dut charon[8866]: 11[ENC] parsed QUICK_MODE request 163731885 [ HASH SA No KE ID ID ]
11:28:24 dut charon[8866]: 11[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
11:28:24 dut charon[8866]: 11[ENC] generating QUICK_MODE response 163731885 [ HASH SA No KE ID ID ]
11:28:24 dut charon[8866]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
11:28:24 dut charon[8866]: 12[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (60 bytes)
11:28:24 dut charon[8866]: 12[ENC] parsed QUICK_MODE request 163731885 [ HASH ]
11:28:24 dut charon[8866]: 12[IKE] CHILD_SA collision-test{1} established with SPIs c3502a7d_i 36e602d2_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:24 dut charon[8866]: 12[IKE] CHILD_SA collision-test{1} established with SPIs c3502a7d_i 36e602d2_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_VERSION=1.1
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_CONNECTION=collision-test
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_MY_PORT=0
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PEER_PROTOCOL=0
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PEER=192.168.252.4
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_VERB=up-client
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PEER_PORT=0
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_ME=192.168.252.131
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PEER_ID=192.168.252.4
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_REQID=1
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_MY_ID=192.168.252.131
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_MY_PROTOCOL=0
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PROTO=esp
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_UNIQUEID=1
11:28:24 dut charon[8866]: 12[CHD] updown: PLUTO_INTERFACE=dp0s2
11:28:32 dut charon[8866]: 12[CFG] vici rekey CHILD_SA #1
11:28:32 dut charon[8866]: 12[ENC] generating QUICK_MODE request 3488210624 [ HASH SA No KE ID ID ]
11:28:32 dut charon[8866]: 12[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)
11:28:32 dut charon[8866]: 07[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
11:28:32 dut charon[8866]: 07[ENC] parsed QUICK_MODE request 1668493352 [ HASH SA No KE ID ID ]
11:28:32 dut charon[8866]: 07[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
11:28:32 dut charon[8866]: 07[IKE] detected rekeying of CHILD_SA collision-test{1}
11:28:32 dut charon[8866]: 07[ENC] generating QUICK_MODE response 1668493352 [ HASH SA No KE ID ID ]
11:28:32 dut charon[8866]: 07[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (380 bytes)

11:28:32 dut charon[8866]: 08[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (364 bytes
)
11:28:32 dut charon[8866]: 08[ENC] parsed QUICK_MODE response 3488210624 [ HASH SA No KE ID ID ]
11:28:32 dut charon[8866]: 08[CFG] selected proposal: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1536/NO_EXT_SEQ
```

```
11:28:32 dut charon[8866]: 08[IKE] CHILD_SA collision-test{2} established with SPIs c8e7f2be_i 7c5346cf_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:32 dut charon[8866]: 08[IKE] CHILD_SA collision-test{2} established with SPIs c8e7f2be_i 7c5346cf_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:32 dut charon[8866]: 08[ENC] generating QUICK_MODE request 3488210624 [ HASH ]
11:28:32 dut charon[8866]: 08[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (60 bytes)
11:28:32 dut charon[8866]: 09[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (60 bytes)
11:28:32 dut charon[8866]: 09[ENC] parsed QUICK_MODE request 1668493352 [ HASH ]
11:28:32 dut charon[8866]: 09[IKE] CHILD_SA collision-test{3} established with SPIs c571a57f_i 4cf9352a_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:32 dut charon[8866]: 09[IKE] CHILD_SA collision-test{3} established with SPIs c571a57f_i 4cf9352a_o and
TS 10.10.3.0/24 === 10.10.1.0/24
11:28:47 dut charon[8866]: 15[NET] received packet: from 192.168.252.4[500] to 192.168.252.131[500] (76 bytes)
11:28:47 dut charon[8866]: 15[ENC] parsed INFORMATIONAL_V1 request 2908304599 [ HASH D ]
11:28:47 dut charon[8866]: 15[IKE] received DELETE for ESP CHILD_SA with SPI 4cf9352a
11:28:47 dut charon[8866]: 15[IKE] detected redundant CHILD_SA collision-test{3}
11:28:47 dut charon[8866]: 15[IKE] closing CHILD_SA collision-test{3} with SPIs c571a57f_i (0 bytes) 4cf9352a_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:28:47 dut charon[8866]: 15[IKE] closing CHILD_SA collision-test{3} with SPIs c571a57f_i (0 bytes) 4cf9352a_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:29:11 dut charon[8866]: 10[CFG] vici terminate IKE_SA 'collision-test'
11:29:11 dut charon[8866]: 11[IKE] closing CHILD_SA collision-test{1} with SPIs c3502a7d_i (0 bytes) 36e602d2_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:29:11 dut charon[8866]: 11[IKE] closing CHILD_SA collision-test{1} with SPIs c3502a7d_i (0 bytes) 36e602d2_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:29:11 dut charon[8866]: 11[IKE] sending DELETE for ESP CHILD_SA with SPI c3502a7d
11:29:11 dut charon[8866]: 11[ENC] generating INFORMATIONAL_V1 request 1369992043 [ HASH D ]
11:29:11 dut charon[8866]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:29:11 dut charon[8866]: 11[IKE] closing CHILD_SA collision-test{2} with SPIs c8e7f2be_i (0 bytes) 7c5346cf_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:29:11 dut charon[8866]: 11[IKE] closing CHILD_SA collision-test{2} with SPIs c8e7f2be_i (0 bytes) 7c5346cf_
o (0 bytes) and TS 10.10.3.0/24 === 10.10.1.0/24
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_VERSION=1.1
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_CONNECTION=collision-test
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_MY_PORT=0
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PEER_PROTOCOL=0
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PEER=192.168.252.4
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_VERB=down-client
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PEER_PORT=0
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_ME=192.168.252.131
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PEER_ID=192.168.252.4
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_REQID=1
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_MY_CLIENT=10.10.3.0/24
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_MY_ID=192.168.252.131
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_MY_PROTOCOL=0
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PROTO=esp
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_PEER_CLIENT=10.10.1.0/24
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_UNIQUEID=1
11:29:11 dut charon[8866]: 11[CHD] updown: PLUTO_INTERFACE=dp0s2
11:29:11 dut charon[8866]: 11[IKE] sending DELETE for ESP CHILD_SA with SPI c8e7f2be
11:29:11 dut charon[8866]: 11[ENC] generating INFORMATIONAL_V1 request 4270418658 [ HASH D ]
11:29:11 dut charon[8866]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (76 bytes)
11:29:11 dut charon[8866]: 11[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
11:29:11 dut charon[8866]: 11[IKE] deleting IKE_SA collision-test[1] between 192.168.252.131[192.168.252.131].
..192.168.252.4[192.168.252.4]
11:29:11 dut charon[8866]: 11[IKE] sending DELETE for IKE_SA collision-test[1]
11:29:11 dut charon[8866]: 11[ENC] generating INFORMATIONAL_V1 request 67370832 [ HASH D ]
11:29:11 dut charon[8866]: 11[NET] sending packet: from 192.168.252.131[500] to 192.168.252.4[500] (92 bytes)
```

Overall the *3060-ikev1-child-rekey-check* branch looks good to me.

Thanks a lot!

#4 - 17.05.2019 12:30 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version set to 5.8.1

I hesitated to mark a redundant Child SA right on it's creation as rekeyed, because I wasn't sure about potential side-effects.

Yes, it's definitely not ideal (nothing related to IKEv1 really is), but it can happen anyway if the timing is different.

> IIUC for the IKEv1 CHILD_SA handling having a CHILD_SA state set to REKEYED probably is just going to influence: updown and close action triggering behavior.

Sounds reasonable.

> Another "special" case would be if charon.delete_rekeyed=yes is set. When marking the redundant CHILD_SA as rekeyed, shouldn't the install() call later also wipe the CHILD_SA which just got marked as "rekeyed"?

The option currently only has an effect on rekeyings as initiator. As responder, the CHILD_SA is left alone until it expires, unless a DELETE is received. (I had a look back and it seems 2f3c08d268 was based on a customer's patch, which also only handled this as initiator; not sure what the exact reasoning for this was, maybe just to leave it up to the initiator - even though IKEv1 deletes are inherently unreliable.)

I guess in this case, keeping the CHILD_SA might actually be preferred, because the other peer could have a totally different view of which CHILD_SA is marked rekeyed (if it does so at all) depending on the timing there.

As you say, this should hopefully be a rare situation.

> I gave e7f8f7da3b1de677a70 a quick try and verified it solves the uneven child-updown for this particular race condition:
> ...
> Overall the *3060-ikev1-child-rekey-check* branch looks good to me.

OK, thanks for testing.

#5 - 22.05.2019 14:01 - Marco Berizzi

Applied this patch to 5.8.0 and everything is fine for me.

```
if (!this->rekey)     {
/* do another check in case SAs were created since we handled      * the QM request, this is consistent with the rekey check      * before installation on the initiator */
check_for_rekeyed_child(this, TRUE);
if (this->rekey)        {
this->child_sa->destroy(this->child_sa);
this->child_sa = child_sa_create(
this->ike_sa->get_my_host(this->ike_sa),
this->ike_sa->get_other_host(this->ike_sa),
this->config, &this->child);
}
}
```

Thanks Tobias.

PS: I hoped to get this fix before 5.8.0 release.

#6 - 22.05.2019 18:31 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed

> Applied this patch to 5.8.0 and everything is fine for me.

Thanks for testing. I've pushed it to master.

> PS: I hoped to get this fix before 5.8.0 release.

It was too close to the release date.