strongSwan - Bug #3644

Charon crashing while passive

01.12.2020 10:15 - Jean-François Hren

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	high availability (ha plugin)		
Target version:	5.9.2		
Affected version:	5.8.1	**Resolution:**	Fixed

Description

Hello,

We stress tested Charon in a cluster configuration by swapping active/passive states between two instances.
A crash occurred randomly on the passive while apparently iterating on the Child SAs of some IKE SA.

After adding more verbose to track add and remove of Child SA from IKE SA, we found an issue.

If an active CHILD_REKEY task is migrated, its CHILD_CREATE subtask is destroyed and the new Child SA is not yet established, this Child SA is destroyed without removing it from its IKE SA leading later to a user-after-free crash.
The task migration occurs because the instance went passive and received an IKE_MID_RESPONDER message for the IKE SA.

Following is a stripped down version of the log for clarity:

```
Nov 30 19:01:34 11[KNL] received an SADB_EXPIRE
Nov 30 19:01:34 11[KNL] creating rekey job for CHILD_SA ESP/0xc9a77d3e/196.0.0.1
Nov 30 19:01:34 12[MGR] checkout IKEv2 SA with SPIs 04ad1a3d11776f2a_i 02a2e9ea26ca9940_r
Nov 30 19:01:34 12[MGR] IKE_SA (3037643136396437313961626461316637316631653334306138313738323634000
)(b23e667f97f9d02208ce532886e326ea)[51] successfully checked out
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> queueing CHILD_REKEY task
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> activating new tasks
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51>   activating CHILD_REKEY task
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> proposing traffic selectors for us:
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51>  101.0.6.90/32
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> proposing traffic selectors for other:
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51>  100.0.6.90/32
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> configured proposals: ESP:AES_GCM_16_256/MODP_2048/NO_EXT_SEQ
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> establishing CHILD_SA (336662313564363936386631353337663563633561653935613238
616461333800)(23b904745dde43c043972de02442e8ef){26052} reqid 1626
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> got SPI cff6264b
[...]
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> CHILD_SA (336662313564363936386631353337663563633561653935613238
616461333800)(23b904745dde43c043972de02442e8ef){22505} state change: INSTALLED => REKEYING
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> Sending HA message 26
[...]
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> generating ENCRYPTED payload finished
Nov 30 19:01:34 12[NET] <(3037643136396437313961626461316637316631653334306138313738323634000)(b23e
667f97f9d02208ce532886e326ea)|51> sending packet: from 196.0.0.1[500] to 196.98.173.17[500] (476 b
```

```
ytes)
Nov 30 19:01:34 12[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin IKE_SA (3037643136396437313961626461316637316631653334306
138313738323634 00)(b23e667f97f9d02208ce532886e326ea)[51]
Nov 30 19:01:34 12[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin of IKE_SA successful
[...]
Nov 30 19:01:34 12[MGR] checkout IKEv2 SA by message with SPIs 04ad1a3d11776f2a_i 02a2e9ea26ca9940
_r
Nov 30 19:01:34 12[MGR] IKE_SA (3037643136396437313961626461316637316631653334306138313738323634 00
)(b23e667f97f9d02208ce532886e326ea)[51] successfully checked out
Nov 30 19:01:34 12[NET] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> received packet: from 196.98.173.17[500] to 196.0.0.1[500] (476
bytes)
[...]
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> parsed CREATE_CHILD_SA response 349 [ N(ESP_TFC_PAD_N) SA No KE
TSi TSr ]
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> selecting proposal:
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   proposal matches
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> received proposals: ESP:AES_GCM_16_256/MODP_2048/NO_EXT_SEQ
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> configured proposals: ESP:AES_GCM_16_256/MODP_2048/NO_EXT_SEQ
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> selected proposal: ESP:AES_GCM_16_256/MODP_2048/NO_EXT_SEQ
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> selecting traffic selectors for us:
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>  config: 101.0.6.90/32, received: 101.0.6.90/32 => match: 101.0.
6.90/32
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> selecting traffic selectors for other:
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>  config: 100.0.6.90/32, received: 100.0.6.90/32 => match: 100.0.
6.90/32
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> CHILD_SA (3366623135643639363866313533376635636335616539356132 38
616461333800)(23b904745dde43c043972de02442e8ef){26052} state change: CREATED => INSTALLING
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   using AES_GCM_16 for encryption
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> adding inbound ESP SA
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   SPI 0xcff6264b, src 196.98.173.17 dst 196.0.0.1
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleting SAD entry with SPI cff6264b
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleted SAD entry with SPI cff6264b
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> adding SAD entry with SPI cff6264b and reqid {1626}
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   using encryption algorithm AES_GCM_16 with key size 288
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> registering outbound ESP SA
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   SPI 0xcd91d885, src 196.0.0.1 dst 196.98.173.17
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> policy 100.0.6.90/32 === 101.0.6.90/32 in already exists, increa
sing refcount
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> handling HA CHILD_SA (3366623135643639363866313533376635636335 61
653935613238616461333800)(23b904745dde43c043972de02442e8ef){26052} 101.0.6.90/32 === 100.0.6.90/32
 (segment in: 1, out: 1)
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
```

```
667f97f9d02208ce532886e326ea)|51> Sending HA message 520
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> inbound CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){26052} established with SPIs cff6264b_i cd91d885_o and TS 101.0.6.90/32 === 100.0.6.90/32
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){26052} state change: INSTALLING => INSTALLED
Nov 30 19:01:34 12[APP] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> IPSEC SA established
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> adding CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){26052}(0x000000080b519f80) cff6264b cd91d885 to (3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)[51]
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> adding outbound ESP SA
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51>   SPI 0xcd91d885, src 196.0.0.1 dst 196.98.173.17
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> adding SAD entry with SPI cd91d885 and reqid {1626}
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51>   using encryption algorithm AES_GCM_16 with key size 288
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> policy 101.0.6.90/32 === 100.0.6.90/32 out already exists, increasing refcount
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> outbound CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){26052} established with SPIs cff6264b_i cd91d885_o and TS 101.0.6.90/32 === 100.0.6.90/32
Nov 30 19:01:34 12[APP] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> sns-auth-sso: no user set, skip SSO
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){22505} state change: REKEYING => REKEYED
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> reinitiating already active tasks
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51>   CHILD_REKEY task
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> going to query SAD entry with SPI c9a77d3e from CHILD SA 0x00000080887aa00
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> querying SAD entry with SPI c9a77d3e
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> going to query SAD entry with SPI c80b861e from CHILD SA 0x00000080887aa00
Nov 30 19:01:34 12[KNL] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> querying SAD entry with SPI c80b861e
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> closing CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){22505} with SPIs c9a77d3e_i (547734 bytes) c80b861e_o (996000 bytes) and TS 101.0.6.90/32 === 100.0.6.90/32
Nov 30 19:01:34 12[APP] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> Closing IPSEC SA
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> added payload of type DELETE to message
Nov 30 19:01:34 12[IKE] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> sending DELETE for ESP CHILD_SA with SPI c9a77d3e
Nov 30 19:01:34 12[CHD] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> CHILD_SA (3366623135643639363866313533376635636335616539356132386164613338
00)(23b904745dde43c043972de02442e8ef){22505} state change: REKEYED => DELETING
Nov 30 19:01:34 12[APP] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> Sending DELETE for IPSEC SA (ESP)
Nov 30 19:01:34 12[CFG] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e667f97f9d02208ce532886e326ea)|51> Sending HA message 26
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634
00)(b23e
```

```
667f97f9d02208ce532886e326ea)|51> order payloads in message
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> added payload of type DELETE to message
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> generating INFORMATIONAL request 350 [ D ]
[...]
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> generating DELETE payload finished
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> generated content in encrypted payload
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> generating payload of type ENCRYPTED
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   generating rule 0 U_INT_8
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   generating rule 1 U_INT_8
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   generating rule 2 PAYLOAD_LENGTH
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51>   generating rule 3 CHUNK_DATA
Nov 30 19:01:34 12[ENC] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> generating ENCRYPTED payload finished
Nov 30 19:01:34 12[NET] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> sending packet: from 196.0.0.1[500] to 196.98.173.17[500] (76 by
tes)
Nov 30 19:01:34 12[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin IKE_SA (3037643136396437313961626461316637316631653334306
138313738323634 00)(b23e667f97f9d02208ce532886e326ea)[51]
Nov 30 19:01:34 15[MGR] checkout IKEv2 SA with SPIs ebcae90698992ea6_i af22a9ad24725f6d_r
Nov 30 19:01:34 12[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin of IKE_SA successful
[...]
Nov 30 19:01:34 06[IKE] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> IKE_SA (3037643136396437313961626461316637316631653334306138313737
3832363400)(b23e667f97f9d02208ce532886e326ea)[51] state change: ESTABLISHED => PASSIVE
[...]
Nov 30 19:01:41 16[CFG] HA message len 26
Nov 30 19:01:41 16[CFG] received HA IKE_MID_RESPONDER message
Nov 30 19:01:41 16[MGR] checkout IKEv2 SA with SPIs 04ad1a3d11776f2a_i 02a2e9ea26ca9940_r
Nov 30 19:01:41 16[MGR] IKE_SA (3037643136396437313961626461316637316631653334306138313738323634 00
)(b23e667f97f9d02208ce532886e326ea)[51] successfully checked out
Nov 30 19:01:41 16[IKE] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> Trying to reset message id
Nov 30 19:01:41 16[IKE] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> Starting to migrate active task CHILD_REKEY
Nov 30 19:01:41 16[CHD] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> CHILD_SA (3366623135643639363866313533376635636335616539356132 38
616461333800)(23b904745dde43c043972de02442e8ef){26052} state change: INSTALLED => DESTROYING
Nov 30 19:01:41 16[APP] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> IPSEC SA deleted
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleting policy 101.0.6.90/32 === 100.0.6.90/32 out
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> policy still used by another CHILD_SA, not removed
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleting policy 100.0.6.90/32 === 101.0.6.90/32 in
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> policy still used by another CHILD_SA, not removed
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleting SAD entry with SPI cff6264b
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleted SAD entry with SPI cff6264b
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleting SAD entry with SPI cd91d885
Nov 30 19:01:41 16[KNL] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> deleted SAD entry with SPI cd91d885
Nov 30 19:01:41 16[IKE] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
```

```
667f97f9d02208ce532886e326ea)|51> Done migrating active task CHILD_REKEY
Nov 30 19:01:41 16[IKE] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> Done resetting message id
Nov 30 19:01:41 16[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin IKE_SA (3037643136396437313961626461316637316631653334306
138313738323634 00)(b23e667f97f9d02208ce532886e326ea)[51]
Nov 30 19:01:41 16[MGR] <(3037643136396437313961626461316637316631653334306138313738323634 00)(b23e
667f97f9d02208ce532886e326ea)|51> checkin of IKE_SA successful
```

Associated revisions

Revision 25ec2d04 - 03.12.2020 11:06 - Tobias Brunner

child-rekey: Don't migrate child-create task if we already are deleting

If we are already deleting the old/redundant CHILD_SA, we must not migrate the child-create task as that would destroy the new CHILD_SA we already moved to the IKE_SA.

Fixes #3644.

History

#1 - 01.12.2020 12:14 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to high availability (ha plugin)

- Status changed from New to Feedback

- Target version set to 5.9.2

> If an active CHILD_REKEY task is migrated, its CHILD_CREATE subtask is destroyed and the new Child SA is not yet established, this Child SA is destroyed without removing it from its IKE SA leading later to a user-after-free crash.

I see, the problem is that the child-rekey task is reused to delete the old SA, while the new SA has already been adopted by the IKE_SA. We should probably avoid migrating the child-create task when we already switched to the deletion stage. I pushed a fix to the *3644-child-rekey-migrate* branch.

#2 - 01.12.2020 16:29 - Jean-François Hren

Tobias Brunner wrote:

> > If an active CHILD_REKEY task is migrated, its CHILD_CREATE subtask is destroyed and the new Child SA is not yet established, this Child SA is destroyed without removing it from its IKE SA leading later to a user-after-free crash.
>
> I see, the problem is that the child-rekey task is reused to delete the old SA, while the new SA has already been adopted by the IKE_SA. We should probably avoid migrating the child-create task when we already switched to the deletion stage. I pushed a fix to the *3644-child-rekey-migrate* branch.

Thank you for the fix. I will test it this night.

#3 - 02.12.2020 08:10 - Jean-François Hren

Jean-François Hren wrote:

> Tobias Brunner wrote:
>
> > If an active CHILD_REKEY task is migrated, its CHILD_CREATE subtask is destroyed and the new Child SA is not yet established, this Child SA is destroyed without removing it from its IKE SA leading later to a user-after-free crash.
>
> I see, the problem is that the child-rekey task is reused to delete the old SA, while the new SA has already been adopted by the IKE_SA. We should probably avoid migrating the child-create task when we already switched to the deletion stage. I pushed a fix to the *3644-child-rekey-migrate* branch.
>
> Thank you for the fix. I will test it this night.

Our stress test produced no crash. Thank you again for the fix.

#4 - 02.12.2020 10:23 - Tobias Brunner

- Assignee set to Tobias Brunner

- Resolution set to Fixed

> Our stress test produced no crash. Thank you again for the fix.

OK, great. I'll line that up for the next release.

#5 - 03.12.2020 11:07 - Tobias Brunner

- Status changed from Feedback to Closed