strongSwan - Bug #752

With fragmentation=yes ikev2 rekeying fails

28.10.2014 08:09 - Volker Rümelin

Status:	Closed	**Start date:**	28.10.2014
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.2.2		
Affected version:	5.2.1	**Resolution:**	Fixed

Description

Hi Tobias,

strongswan 5.2.1 ikev2 rekeying fails if the CREATE_CHILD_SA request is sent as fragments.

```
ipsec.conf:
conn home-online
        keyexchange=ikev2
        keyingtries=%forever
        dpdaction=restart
        leftsubnet=87.x.x.x/32,2001:x:x:0::/64
        right=212.x.x.x
        rightsubnet=212.x.x.x/32,2001:x:x:10::/64
        rightid="@sun.example.com"
        ike=aes256-sha2_256-modp2048,aes128-sha1-modp2048!
        esp=aes256-sha2_256-modp2048,aes128-sha1-modp2048!
        mobike=no
        fragmentation=yes
        auto=start

Initiator log:
Oct 27 22:42:36 srv charon: 09[KNL] creating rekey job for ESP CHILD_SA with SPI cb3091e1 and reqi
d {5}
Oct 27 22:42:36 srv charon: 09[IKE] establishing CHILD_SA home-online{5}
Oct 27 22:42:36 srv charon: 09[ENC] generating CREATE_CHILD_SA request 2 [ N(REKEY_SA) SA No KE TS
i TSr ]
Oct 27 22:42:36 srv charon: 09[ENC] splitting IKE message with length of 608 bytes into 2 fragment
s
Oct 27 22:42:36 srv charon: 09[ENC] payload ENCRYPTED_FRAGMENT has no ordering rule in CREATE_CHIL
D_SA request
Oct 27 22:42:36 srv charon: 09[ENC] generating CREATE_CHILD_SA request 2 [ EF ]
Oct 27 22:42:36 srv charon: 09[ENC] payload ENCRYPTED_FRAGMENT has no ordering rule in CREATE_CHIL
D_SA request
Oct 27 22:42:36 srv charon: 09[ENC] generating CREATE_CHILD_SA request 2 [ EF ]
Oct 27 22:42:36 srv charon: 09[NET] sending packet: from 87.x.x.x[500] to 212.x.x.x[500] (548 byte
s)
Oct 27 22:42:36 srv charon: 09[NET] sending packet: from 87.x.x.x[500] to 212.x.x.x[500] (132 byte
s)
Oct 27 22:42:36 srv charon: 11[NET] received packet: from 212.x.x.x[500] to 87.x.x.x[500] (80 byte
s)
Oct 27 22:42:36 srv charon: 11[ENC] parsed CREATE_CHILD_SA response 2 [ N(INVAL_SYN) ]
Oct 27 22:42:36 srv charon: 11[IKE] received INVALID_SYNTAX notify error
Oct 27 22:42:36 srv charon: 11[IKE] CHILD_SA rekeying failed, trying again in 15 seconds
Oct 27 22:42:36 srv charon: 08[NET] received packet: from 212.x.x.x[500] to 87.x.x.x[500] (80 byte
s)
Oct 27 22:42:36 srv charon: 08[ENC] parsed CREATE_CHILD_SA response 2 [ N(INVAL_SYN) ]
Oct 27 22:42:36 srv charon: 08[IKE] received message ID 2, expected 3. Ignored

Responder log:
Oct 27 22:42:36 sun charon: 10[NET] received packet: from 87.x.x.x[500] to 212.x.x.x[500] (548 byt
es)
Oct 27 22:42:36 sun charon: 10[ENC] payload of type SECURITY_ASSOCIATION not occurred 1 times (0)
```

```
Oct 27 22:42:36 sun charon: 10[IKE] message verification failed
Oct 27 22:42:36 sun charon: 10[ENC] generating CREATE_CHILD_SA response 2 [ N(INVAL_SYN) ]
Oct 27 22:42:36 sun charon: 10[NET] sending packet: from 212.x.x.x[500] to 87.x.x.x[500] (80 bytes
)
Oct 27 22:42:36 sun charon: 10[IKE] CREATE_CHILD_SA request with message ID 2 processing failed
Oct 27 22:42:36 sun charon: 03[NET] received packet: from 87.x.x.x[500] to 212.x.x.x[500] (132 byt
es)
Oct 27 22:42:36 sun charon: 03[ENC] payload of type SECURITY_ASSOCIATION not occurred 1 times (0)
Oct 27 22:42:36 sun charon: 03[IKE] message verification failed
Oct 27 22:42:36 sun charon: 03[ENC] generating CREATE_CHILD_SA response 2 [ N(INVAL_SYN) ]
Oct 27 22:42:36 sun charon: 03[NET] sending packet: from 212.x.x.x[500] to 87.x.x.x[500] (80 bytes
)
Oct 27 22:42:36 sun charon: 03[IKE] CREATE_CHILD_SA request with message ID 2 processing failed
```

Regards,
Volker

Associated revisions

Revision b0891697 - 29.10.2014 15:51 - Tobias Brunner

message: Include encrypted fragment payload in payload (order) rules

Otherwise fragmented CREATE_CHILD_SA exchanges won't get accepted
because they don't contain an SA payload.

It also prevents a warning when ordering payloads.

Fixes #752.

History

#1 - 28.10.2014 16:57 - Tobias Brunner

- Status changed from New to Feedback

- Assignee set to Tobias Brunner

- Target version set to 5.2.2

Thanks for the report.

While encrypted fragment payloads are mostly handled like encrypted payloads, they are in some cases treated like regular payloads. Unfortunately, I missed to update the arrays that define the payload ordering and the allowed payloads for each exchange. This isn't a problem for IKE_AUTH as it has no mandatory payloads defined (the only issue there is the warning regarding payload ordering, which I never noticed for some reason). On the other hand, we require certain payloads in a CREATE_CHILD_SA exchange and therefore processing fails if the only payload found is an encrypted fragment. The patch in the *frag-rekey* branch should fix the problem.

#2 - 29.10.2014 08:19 - Volker Rümelin

Yes, your patch fixes the problem.

#3 - 29.10.2014 15:56 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

#4 - 29.10.2014 15:56 - Tobias Brunner

Thanks for testing!