strongSwan - Issue #3527

INFORMATIONAL DELETE response to CHILD_SA contains IPSec_SA SPI and IKE DELETE payloads. Strongswan does not delete IKE SA policy from kernel.

27.07.2020 18:34 - Scott Sussman

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.8.4	**Resolution:**	No feedback

Description

Hello,

We have a scenario where we (the responder) send an INFORMATIONAL DELETE request for a CHILD_SA to the client (initiator).

The response fails integrity check and contains an incorrect flag set to responder even though the response is from the initiator so strongSwan retransmits the CHILD_SA INFORMATIONAL DELETE.

The response to the retransmitted INFORMATIONAL DELETE contains 2 payloads,

- the first is a DELETE for the IPSec_SA SPI and
- the second is the IKE DELETE payload.

We expected the CHILD_SA SPI only in the retransmit response that is associated with the CHILD_SA from the request.

After processing this response packet we are left with the IKE established while the IPSec_SA and initially requested CHILD_SA are removed.
Is the client (initiator) response valid and if so why is strongSwan not removing the IKE and only removing the IPSec_SA and all the CHILD_SA's?

I have attached a decoded text trace of the exchange. Some parts of IKE AUTH have been removed for brevity.

Packet #16126 Initiator Request IPSec SA SPI 0000048d
Packet #16163 Responder Response IPSec SA SPI c255cd60

Packet #332264 Responder Request Child SA Create SPI c7b9b0dd
Packet #332269 Initiator Response Child SA Create SPI 000079bd

Packet #543209 Responder Request INFORMATIONAL DELETE Child SA SPI c7b9b0dd
Packet #543210 Initiator Response with Integrity check failure and incorrect flag set as RESPONDER for INITIATOR sent packet.

Packet #548806 Responder Request retransmit INFORMATIONAL DELETE Child SA SPI c7b9b0dd
Packet #548807 Initiator Response retransmit INFORMATIONAL DELETE reply with IPSec SA SPI 0000048d and IKE DELETE. <-- is this a valid response to the CHILD SA DELETE?

After the exchange the ipsec statusall on the responder side still contains the IKE SA:

```
Connections:
        casa:  10.42.192.175...%any  IKEv1/2
        casa:   local:  [%any] uses pre-shared key authentication
        casa:   remote: [%any] uses EAP authentication
         net:   child:  10.42.192.175/32[tcp/38413] === dynamic TUNNEL
        net1:   child:  10.43.155.203/32 === dynamic TUNNEL
Security Associations (1 up, 0 connecting):
        casa[910]: ESTABLISHED 24 minutes ago, 10.42.192.175[10.42.192.175]...10.42.192.142[34.14.
4.36]
        casa[910]: IKEv2 SPIs: 1602d86c00000000_i 4b89efb88fed0130_r*, rekeying disabled
        casa[910]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_2048
```

History

#1 - 28.07.2020 10:00 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

Please add the strongSwan logs (see HelpRequests). What strongSwan version are you using?

#2 - 02.10.2020 10:30 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No feedback

Files

pdu-delete-issue.txt	66.2 KB	27.07.2020	Scott Sussman