strongSwan - Issue #2731

IKEv2 rekey uses KE of wrong DH group

27.08.2018 18:22 - Paul Wouters

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	android		
Affected version:	5.6.1	**Resolution:**	Can't reproduce

Description

strongswan initiates to libreswan, with a KE for ECP_256.
libreswan sends INVALID_KE with MODP2048 group
strongswan resends IKE_INIT with proper KE.
IKE SA and IPsec SA establish

then strongswan comes back an hour later for rekey using a KE payload for CURVE25519. This DH group was never in any of the proposals in the initial exchanges.

libreswan replies with INVALID_KE

strongswan resends message with MSGID 3 of same length (so presumably did not change its KE payload).

libreswan sees this as a retransmit

the connection ends up failing

I believe there are at least two bugs here:

- strongswan, if it is willing to do different DH groups on rekey (instead of insisting on keeping the DH the same) should at least default to using the DH group that was used before, and guess the KE payload belonging to that group
- strongswan should never pick a DH/KE for rekey that was not part of the original transform set of the responder for the initial exchange

And I *think* there is a third bug here, but I can't find the RFC text to prove it

- when receiving INVALID_KE on msgid 3, I think the next REKEY attempt via CREATE_CHILD_SA should use msgid 4. But strongswan uses msgid 3

History

#1 - 28.08.2018 09:03 - Tobias Brunner

- Status changed from New to Feedback

> then strongswan comes back an hour later for rekey using a KE payload for CURVE25519. This DH group was never in any of the proposals in the initial exchanges.

Sounds strange.

> libreswan replies with INVALID_KE
>
> strongswan resends message with MSGID 3 of same length (so presumably did not change its KE payload).

That does sound like a retransmit. Check the strongSwan log to see if it actually received the message with the INVALID_KE notify. Also, what was the message with MID 2? DPD? CHILD_SA rekey?

> I believe there are at least two bugs here:
>
> - strongswan, if it is willing to do different DH groups on rekey (instead of insisting on keeping the DH the same) should at least default to using the DH group that was used before, and guess the KE payload belonging to that group

That should be the case since #2526 (included in 5.6.2). Did you actually use 5.6.3 (see "affected version") for this test?

> - strongswan should never pick a DH/KE for rekey that was not part of the original transform set of the responder for the initial exchange

That really sounds strange, never seen it reported before. Are you sure it was not part of the original proposal? (Although, I don't see a reason why the group should switch from the originally selected ECP_256 even then.) Did you explicitly configure the IKE proposal in the config?

> And I *think* there is a third bug here, but I can't find the RFC text to prove it
>
> - when receiving INVALID_KE on msgid 3, I think the next REKEY attempt via CREATE_CHILD_SA should use msgid 4. But strongswan uses msgid 3

It should, and in my tests it does. Unless it's a retransmit, as mentioned above.

By the way, do you still have that PPK test server running you once mentioned on the ipsecme mailing list? The IP resolves fine, but there is no response to IKE_SA_INIT requests.

#2 - 28.08.2018 17:51 - Paul Wouters

I heard back from the client side. This was using the strongswan SDK for Android. Apparently this was build over a year ago, so probably older then 5.6.2

Let me clarify:

```
- strongswan should never pick a DH/KE for rekey that was not part of the original transform set of the respon
der for the initial exchange
```

I meant to say that the responder (libreswan) did not contain curve25519. The strongswan/initiator did. But I still think it should not pick a KE that was previously confirmed to have zero chance of success.

I do believe the msgid 3 was a retransmit as the size was identical. I don't have client logs and the libreswan server didn't re-parse it because it assumed this was a retransmit.

(ppk server was down, i restarted it. please ping me via email if you want me to check logs etc)

#3 - 29.08.2018 10:40 - Tobias Brunner

- Affected version changed from 5.6.3 to 5.6.1

> I heard back from the client side. This was using the strongswan SDK for Android. Apparently this was build over a year ago, so probably older then 5.6.2

I see. The code around a year ago was probably based on 5.6.0 or 5.6.1. The exact commit they used as their base would help (as well as possible code changes they applied).

> Let me clarify:
>
> - strongswan should never pick a DH/KE for rekey that was not part of the original transform set of the responder for the initial exchange
>
> I meant to say that the responder (libreswan) did not contain curve25519. The strongswan/initiator did. But I still think it should not pick a KE that was previously confirmed to have zero chance of success.

We can't know that. The only thing we get back from the responder is the selected proposal (i.e. exactly one DH group). We won't ever see what other groups it supports/has configured (that would require an ike-scan like approach of trying different single proposals). While I agree it's not that likely that the DH group will change during a rekeying (which is why we now propose the previous group first and in the KE payload), it's still theoretically possible, so we don't deny the responder the possibility to select a different DH group and propose the other configured/supported groups too.

Why the initiator would select a different group than it originally did (i.e. the switch from ecp256 to curve25519), I don't know. That's definitely strange, the client log might have something about this.

> I do believe the msgid 3 was a retransmit as the size was identical. I don't have client logs and the libreswan server didn't re-parse it because it assumed this was a retransmit.

I'd expect it to be a retransmit too, I don't see how else this could happen.

> (ppk server was down, i restarted it. please ping me via email if you want me to check logs etc)

Thanks, I'll send you an email with my test results.

#4 - 21.05.2019 11:57 - Tobias Brunner

- Category changed from charon to android

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Can't reproduce