strongSwan - Bug #1478

ikeOutInitRsp counter is twice than ikeInInitReq

24.05.2016 16:48 - Danny Kulchinsky

Status:	Closed	**Start date:**	24.05.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.5.0		
Affected version:	5.3.5	**Resolution:**	Fixed

Description

strongSwan is setup as responder for road-warriers with eap-radius authentication.

I'm looking at the output of "ipsec listcounters" and something is strange with ikeInInitReq (1009046) and ikeOutInitRsp (2018092) - why are there twice Responses than Requests ?

By reviewing the logs we see that number of IKE_SA_INIT Requests and Responses are identical...

```
# ipsec listcounters

List of IKE counters:

ikeInitRekey               3083
ikeRspRekey                   0
ikeChildSaRekey             159
ikeInInvalid              37027
ikeInInvalidSpi          373716
*ikeInInitReq            1009046*
ikeInInitRsp                  0
ikeOutInitReq                 0
*ikeOutInitRsp           2018092*
ikeInAuthReq            2144571
ikeInAuthRsp                  0
ikeOutAuthReq                 0
ikeOutAuthRsp           2144565
ikeInCrChildReq             159
ikeInCrChildRsp            3083
ikeOutCrChildReq           3095
ikeOutCrChildRsp            159
ikeInInfoReq            4843345
ikeInInfoRsp            5479160
ikeOutInfoReq           5603133
ikeOutInfoRsp           4843345
```

Any ideas ? am I missing something ?

Thanks,
Danny

Associated revisions

Revision e35bb6e9 - 06.06.2016 14:12 - Tobias Brunner

ike: Don't trigger message hook when fragmenting pre-generated messages

This is the case for the IKE_SA_INIT and the initial IKEv1 messages, which
are pre-generated in tasks as at least parts of it are used to generate
the AUTH payload. The IKE_SA_INIT message will never be fragmented, but
the IKEv1 messages might be, so we can't just call generate_message().

Fixes #1478.

History

#1 - 24.05.2016 19:15 - Tobias Brunner

- Description updated

- Status changed from New to Feedback

I can't reproduce this. Anything special in your setup? Configuration? Custom plugins? Code modifications?

#2 - 24.05.2016 19:35 - Danny Kulchinsky

Tobias Brunner wrote:

> I can't reproduce this. Anything special in your setup? Configuration? Custom plugins? Code modifications?

No custom code/plugins, nothing special I can think of.

This is our ipsec.conf:

```
config setup

conn %default
    ikelifetime=8h
    keylife=24h
    rekeymargin=9m
    keyingtries=1
    keyexchange=ikev2

    dpdaction=clear
    dpddelay=60s

    fragmentation=yes

    ike=aes256-md5-sha1-modp1024!

    esp=aes256-md5!

    reauth=no

conn XXX-XXXXXX
    # left - local (server) side
    left=%any
    leftid=XYZ
    leftauth=eap
    leftsubnet=y.y.y.y/24
    leftcert=vpnHostCert.der
    leftfirewall=yes

    # right - remote (client) side
    right=%any
    rightid=%any
    rightsendcert=never
    rightauth=eap-radius
    rightsourceip=x.x.x.x/16
    auto=add
```

#3 - 25.05.2016 10:34 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to libcharon

- Assignee set to Tobias Brunner

- Target version set to 5.5.0

Ah, I see. It's related to *fragmentation=yes*. The IKE_SA_INIT response is pre-generated by the task that later handles the IKE_AUTH message (the contents of the IKE_SA_INIT response are used when calculating the value of the AUTH payload): source:src/libcharon/sa/ikev2/tasks/ike_auth.c#L154. This triggers the message hook, which is used by the *stroke* plugin to count messages. In the called method there is a check, so that the message isn't generated again if it already was: source:src/libcharon/sa/ike_sa.c#L1173. However, when generating the actual response we now call ike_sa_t::generate_message_fragmented, which will call ike_sa_t::generate_message in case IKE fragmentation is disabled or not supported, but otherwise generates the message directly, triggering the message hook again.

I pushed a fix to the *1478-pre-generated-no-hooks* branch, which avoids triggering the message hook if the message was already pre-generated.

#4 - 25.05.2016 11:15 - Danny Kulchinsky

Tobias Brunner wrote:

> Ah, I see. It's related to *fragmentation=yes*. The IKE_SA_INIT response is pre-generated by the task that later handles the IKE_AUTH message (the contents of the IKE_SA_INIT response are used when calculating the value of the AUTH payload): source:src/libcharon/sa/ikev2/tasks/ike_auth.c#L154. This triggers the message hook, which is used by the *stroke* plugin to count messages. In the called method there is a check, so that the message isn't generated again if it already was: source:src/libcharon/sa/ike_sa.c#L1173. However, when generating the actual response we now call ike_sa_t::generate_message_fragmented, which will call ike_sa_t::generate_message in case IKE fragmentation is disabled or not supported, but otherwise generates the message directly, triggering the message hook again.
>
> I pushed a fix to the *1478-pre-generated-no-hooks* branch, which avoids triggering the message hook if the message was already pre-generated.

Thanks so much Tobias!

We'll wait for 5.4.1 and upgrade once available.

Best Regards,
Danny

#5 - 06.06.2016 14:13 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed