strongSwan - Bug #1077

IKEv1 StrongSwan-to-Racoon connections failing when initiator posseses an ECDSA cert

19.08.2015 17:02 - J. Bill Chilton

Status:	Closed	**Start date:**	19.08.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.3.3		
Affected version:	5.3.0	**Resolution:**	Fixed

Description

I'm doing tests w/ Charon configured to initiate IKEv2 StrongSwan-to-StrongSwan connections with ECDSA certs, and IKEv1 connections to older Racoon systems with RSA certs.

I'm seeing the IKEv1 connections fail because the Racoon responders reject the SA proposals they get because they don't know Authentication Method "10" (ECDSA). This despite having an RSA certificate specified in the initiator's swanctl.conf connections.<conn>.local section for that responder.

Tellingly, it only fails when the initiator's credentials have been loaded in such a way that its ECDSA cert comes before its RSA cert in the output produced by swanctl --list-certs.

Now I'm in a little over my head here, but I'm wondering why line 407 of src/libcharon/sa/ikev1/phase1.c:

```
private = lib->credmgr->get_private(lib->credmgr, KEY_ANY, id, NULL);
```

passes NULL as the auth_cfg_t *auth argument to get_private().

Changing "NULL" to "auth" there seems to result in the behavior I expected, with the cert specified in the Racoon system's connections.<conn>.local section apparently determining which Authentication Method is proposed.

Associated revisions

Revision 47ee6017 - 19.08.2015 17:39 - Tobias Brunner

ikev1: Pass current auth-cfg when looking for key to determine auth method

If multiple certificates use the same subjects we might choose the wrong one otherwise. This way we use the one referenced with leftcert and stored in the auth-cfg and we actually do the same thing later in the pubkey authenticator.

Fixes #1077.

Revision 904f93f6 - 03.03.2016 17:26 - Tobias Brunner

ikev1: Avoid modifying local auth config when detecting pubkey method

If it was necessary to pass the local certificates we could probably clone the config (but we don't do that either when later looking for the key to actually authenticate).
Passing auth adds the same subject cert to the config over and over again (I guess we could also try to prevent that by searching for duplicates).

History

#1 - 19.08.2015 17:21 - Tobias Brunner

- Tracker changed from Issue to Bug

- Status changed from New to Feedback

- % Done set to 0

> Tellingly, it only fails when the initiator's credentials have been loaded in such a way that its ECDSA cert comes before its RSA cert in the output

> produced by swanctl --list-certs.

If the certificates have the same identity that's an obvious side-effect of the code below, the first certificate with that ID will be used.

> Now I'm in a little over my head here, but I'm wondering why line 407 of src/libcharon/sa/ikev1/phase1.c:
>
> private = lib->credmgr->get_private(lib->credmgr, KEY_ANY, id, NULL);
>
> passes NULL as the auth_cfg_t *auth argument to get_private().
>
> Changing "NULL" to "auth" there seems to result in the behavior I expected, with the cert specified in the Racoon system's connections.<conn>.local section apparently determining which Authentication Method is proposed.

Yes, quite interesting. It's been like this ever since it was added, not sure what the reason behind it is, but passing auth seems reasonable to me. I'll run the test suite but if nothing shows up I'll push that to master.

Thanks for the report and analysis.

#2 - 19.08.2015 18:01 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.3.3

- Resolution set to Fixed

Applied to master.