

strongSwan - Bug #2954

The inactivity parameter changes the start_action

06.03.2019 16:43 - Alexander Vasiliev

Status:	Closed	Start date:	06.03.2019
Priority:	Normal	Due date:	
Assignee:	Tobias Brunner	Estimated time:	0.00 hour
Category:	vici		
Target version:	5.8.0		
Affected version:	5.7.2	Resolution:	Fixed
Description			
<p>Hi. I dont know if this is a bug but when i've got this behavior i was confused. Also i didnt find any info in wiki or man pages. When i run strongswan-swanctl.service with this in swanctl.conf:</p> <pre>inactivity = 300s close_action = trap start_action = trap</pre> <p>it ends up with this in logs (and this is what i expect to see):</p> <pre>... Wed, 2019-03-06 18:26 09[CFG] conn to-881: Wed, 2019-03-06 18:26 09[CFG] child to-881: ... Wed, 2019-03-06 18:26 09[CFG] start_action = hold Wed, 2019-03-06 18:26 09[CFG] close_action = hold ... Wed, 2019-03-06 18:26 09[CFG] inactivity = 300 ...</pre> <p>But if i will put inactivity after actions:</p> <pre>close_action = trap start_action = trap inactivity = 300s</pre> <pre>... Wed, 2019-03-06 18:32 08[CFG] conn to-881: Wed, 2019-03-06 18:32 08[CFG] child to-881: ... Wed, 2019-03-06 18:32 08[CFG] start_action = clear Wed, 2019-03-06 18:32 08[CFG] close_action = hold ... Wed, 2019-03-06 18:32 08[CFG] inactivity = 300 ...</pre> <p>as a result there is no installed routes and policies. May be this is "by design" but there are no any notes on a strict order of options.</p> <p>Thanks, Alex PS. I am sorry for my english</p>			

Associated revisions

Revision 090e2cf5 - 08.03.2019 15:47 - Tobias Brunner

vici: Correctly parse inactivity timeout as uint32_t

Using parse_time() directly actually overwrites the next member in the child_cfg_create_t struct, which is start_action, which can cause incorrect configs if inactivity is parsed after start_action.

Fixes #2954.

History

#1 - 06.03.2019 18:46 - Tobias Brunner

- Category changed from *swanctl* to *vici*
- Status changed from *New* to *Feedback*
- Assignee set to *Tobias Brunner*
- Target version set to *5.8.0*
- Resolution set to *Fixed*

The order of the options obviously should not matter. So it's definitely a bug.

The *vici* plugin parses the value of the *inactivity* option using the *parse_time()* utility function, which expects a pointer to a *uint64_t*. However, the struct member for *inactivity*, whose pointer is passed, is only a *uint32_t*. So writing to it also affects the struct member that follows it, which is, you can probably guess, *start_action*. So only if *start_action* is parsed after *inactivity* will it work as that corrects this side-effect.

I pushed a fix for this to the *2954-vici-inactivity* branch.

By the way, *close_action=trap* is not needed if you already have *start_action=trap*.

#2 - 07.03.2019 08:51 - Alexander Vasiliev

I pushed a fix for this to the *2954-vici-inactivity* branch.

Great. Thank you

By the way, *close_action=trap* is not needed if you already have *start_action=trap*.

Ok. I am new in this IPsec and StrongSwan world. So was trying things and got stucked with this.

Thanks again.

#3 - 08.03.2019 15:48 - Tobias Brunner

- Status changed from *Feedback* to *Closed*