strongSwan - Bug #3192

RFC 4555 ADDITIONAL_IP6_ADDRESS notifications sent for temporary & deprecated IPv6 addresses

03.10.2019 20:03 - Christian U

Status:	Closed	**Start date:**	03.10.2019
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	kernel-interface		
Target version:	5.8.2		
Affected version:	5.8.1	**Resolution:**	Fixed

Description

Hello,

in our network we have properly implemented IPv6 privacy extensions, which generate a new outgoing temporary address about every 10 minutes. So by design we have many IPv6 addresses on our public interface with a preferred lifetime of zero, but a positive valid lifetime. The kernel correctly flags those as deprecated. A public DNS entry points to the non-temporary IPv6 address of a strongSwan responder instance.

For some reason strongSwan publishes many deprecated IPv6 addresses with N(ADD_6_ADDR) notifications to its peers, within IKE_AUTH responses and INFORMATIONAL requests:

N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR)]
Oct 3 12:55:21 firewall charon-systemd[4971]: generating INFORMATIONAL request 0 [N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR)]
Oct 3 15:58:55 firewall charon-systemd[4971]: generating IKE_AUTH response 1 [IDr CERT AUTH CPRP(ADDR DNS) SA TSi TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR)]

Expected behaviour: strongSwan should not announce deprecated addresses (especially if strongSwan has never used them for communication). Ideally it should not announce temporary addresses at all, but that could be optional.

Associated revisions

Revision b3db3617 - 22.10.2019 14:55 - Tobias Brunner

Merge branch 'ipv6-addrs-mobike'

Address enumeration on Linux now ignores deprecated addresses and
whether temporary or permanent IPv6 addresses are included now depends
on the charon.prefer_temporary_addrs setting.

Closes #3192.

History

#1 - 04.10.2019 10:48 - Tobias Brunner

- Category changed from charon to kernel-interface

- Status changed from New to Feedback

- Target version set to 5.8.2

> For some reason strongSwan publishes many deprecated IPv6 addresses with N(ADD_6_ADDR) notifications to its peers, within IKE_AUTH responses and INFORMATIONAL requests:

These are for MOBIKE.

> Expected behaviour: strongSwan should not announce deprecated addresses (especially if strongSwan has never used them for communication). Ideally it should not announce temporary addresses at all, but that could be optional.

I agree that sending deprecated addresses (or considering them for other purposes) doesn't make sense. I've pushed a fix for that to the *3192-ipv6-addrs* branch. I guess temporary addresses could actually be used, though (with regular MOBIKE updates). Maybe we could use the

existing *charon.prefer_temporary_addrs* option (disabled by default, and currently used for source address selection) to decide whether to enumerate either temporary or permanent addresses. What do you think?

#2 - 04.10.2019 12:07 - Christian U

Tobias Brunner wrote:

> I guess temporary addresses could actually be used, though (with regular MOBIKE updates). Maybe we could use the existing *charon.prefer_temporary_addrs* option (disabled by default, and currently used for source address selection) to decide whether to enumerate either temporary or permanent addresses. What do you think?

That's a good idea. There are certainly scenarios, where using temporary addresses would make sense, especially from an initiator perspective. By enabling *charon.prefer_temporary_addrs* the user would express that intent, and thus notifying about temporary addresses would be the right thing to do in that case (and sticking to permanent ones if disabled).

Thank you for the quick fix and, BTW, for such an extensive and high-quality product. Two weeks ago I have fought again 2 days trying to make the new RHEL8 supported LibreSwan do the same things and eventually gave up. Replaced it with strongSwan from source. Build is super clean, systemd-integration is flawless out of the box, and the swanctl-variant a beauty to setup. I use it with AES_GCM_16_128/PRF_HMAC_SHA2_256/CURVE_25519 for Apple iOS roadwarriors and it works like a charm.

#3 - 04.10.2019 15:59 - Tobias Brunner

> That's a good idea. There are certainly scenarios, where using temporary addresses would make sense, especially from an initiator perspective. By enabling *charon.prefer_temporary_addrs* the user would express that intent, and thus notifying about temporary addresses would be the right thing to do in that case (and sticking to permanent ones if disabled).

I've pushed another commit to the branch. I wonder if it's too restrictive like that (only temporary addresses are sent if the option is enabled, only permanent ones if it is disabled), but I suppose one usually wants to use one or the other, not a mix of both.

> Build is super clean, systemd-integration is flawless out of the box, and the swanctl-variant a beauty to setup. I use it with AES_GCM_16_128/PRF_HMAC_SHA2_256/CURVE_25519 for Apple iOS roadwarriors and it works like a charm.

Nice to hear :)

#4 - 09.10.2019 20:43 - Christian U

I have patched *kernel_netlink_net.c* in 5.8.1 with your changes and can confirm it to be working as expected. Thank you!

#5 - 10.10.2019 15:55 - Tobias Brunner

- Assignee set to Tobias Brunner

- Resolution set to Fixed

> I have patched *kernel_netlink_net.c* in 5.8.1 with your changes and can confirm it to be working as expected. Thank you!

Great, thanks for testing. Will be included in the next release.

#6 - 22.10.2019 14:56 - Tobias Brunner

- Status changed from Feedback to Closed