

strongSwan - Bug #598

Wrong source IPv6 address selection for virtual address and split-tunnel

22.05.2014 00:44 - Ruslan Marchenko

Status:	Closed	Start date:	22.05.2014
Priority:	Normal	Due date:	
Assignee:	Tobias Brunner	Estimated time:	0.00 hour
Category:	libhydra	Resolution:	Fixed
Target version:	5.2.0		
Affected version:	5.1.3		
Description			
Hi, When rw receives address to install, that address is appended to the interface with global scope and indefinite lifetime. This causes the address to be used by non-ipsec traffic - which definitely fails. To mitigate this an address should be marked as invalid for rfc sort. For ipsec traffic source is assigned explicitly by rule so address validity is irrelevant. Proposed patch sets preferred lifetime for an address to 0 which immediately deprecates the address. This exempts the address from normal src selection by IPv6 stack implementation. Regards, Ruslan			
Related issues:			
Related to Issue #694: IPv6 address assigned via CPREQ(ADDR6) is set to "depr...			Closed

Associated revisions

Revision 90854d28 - 20.06.2014 16:10 - Tobias Brunner

kernel-netlink: Install virtual IPv6 addresses as deprecated

This should prevent the kernel's IPv6 source address selection algorithm from using this address unless it is forced to by our source route. This is helpful if split tunneling is used.

Fixes #598.

History

#1 - 20.06.2014 16:14 - Tobias Brunner

- Tracker changed from Issue to Bug
- Category set to libhydra
- Status changed from New to Closed
- Assignee set to Tobias Brunner
- Target version set to 5.2.0
- Resolution set to Fixed

Thanks for the report. I pushed a modified version of your patch to our repository (see associated commit).

As a workaround you could try to set `charon.install_virtual_ip_on` in strongswan.conf to e.g. `lo` (by default virtual IPs are installed on the outbound interface), which should also prevent the kernel from choosing these addresses.

#2 - 03.04.2018 15:24 - Tobias Brunner

- Related to Issue #694: IPv6 address assigned via CPREQ(ADDR6) is set to "deprecated", preferred_lft 0sec added

Files

0001-Fix-wrong-source-address-selection-problem-for-IPv6-.patch	1.33 KB	21.05.2014	Ruslan Marchenko
-----------------------------------------------------------------	---------	------------	------------------