strongSwan - Bug #1174

NULL encryption broken (again) since version 5.3

23.10.2015 12:15 - Peter Whisker

Status:	Closed	**Start date:**	23.10.2015
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.3.4		
Affected version:	5.3.3	**Resolution:**	Fixed

Description

Changes to the sources since 5.3 (ie 5.3.1,.2,.3) seem to have broken kernel-libipsec with NULL encryption as follows:

We are trying to run kernel-libipsec with null esp encryption using strongswan 5.3.2 on Centos 7.

When it attempt to setup the child SA we get the following error in the logs

Oct 21 14:06:54 irisp-asgw-2 charon: 04[CFG] selecting traffic selectors for other:
Oct 21 14:06:54 irisp-asgw-2 charon: 04[CFG] config: 10.10.0.0/24, received: 10.10.0.0/24 => match: 10.10.0.0/24
Oct 21 14:06:54 irisp-asgw-2 charon: 04[ESP] failed to create ESP context: creating iv gen failed
Oct 21 14:06:54 irisp-asgw-2 charon: 04[ESP] failed to create SAD entry
Oct 21 14:06:54 irisp-asgw-2 charon: 04[ESP] failed to create ESP context: creating iv gen failed
Oct 21 14:06:54 irisp-asgw-2 charon: 04[ESP] failed to create SAD entry
Oct 21 14:06:54 irisp-asgw-2 charon: 04[IKE] unable to install inbound and outbound IPsec SA (SAD) in kernel
Oct 21 14:06:54 irisp-asgw-2 charon: 04[IKE] failed to establish CHILD_SA, keeping IKE_SA

This appears to come from around line 279 of src/libipsec/esp_context.c as the table called to return the iv generator does not have one for NULL encryption. Which is what I'd expect for NULL encryption, but I'm, no expert on that level of detail.

The problem is resolved if we enable encryption for ESP but we want to run with NULL.

We have tried it on Debian also (to rule out openssl issues).

We are stuck having to use NULL encryption in this application - StrongSwan is being used solely for ensuring integrity as the data content is not sensitive but needs to be guaranteed also data forensics require easy-to-read content logs!

Peter

Associated revisions

Revision 4fc0a9d4 - 09.11.2015 11:16 - Tobias Brunner

Merge branch 'iv-gen-null-encr'

Fixes NULL encryption in libipsec.

Fixes #1174.

History

#1 - 23.10.2015 14:50 - Tobias Brunner

- Status changed from New to Feedback

> This appears to come from around line 279 of src/libipsec/esp_context.c as the table called to return the iv generator does not have one for NULL encryption. Which is what I'd expect for NULL encryption, but I'm, no expert on that level of detail.

Correct, NULL encryption obviously does not need an IV (this was the problem with #854, i.e. that the IV length returned by the crypter_t implementation was not 0 but the block size). So we could either check the IV length and change some of the code that currently relies on the IV generator to be defined, or we simply create an IV generator that doesn't actually allocate an IV (and only accepts requests for 0 length IVs), which handles this transparently for the current code. I implemented the latter in the *1174-iv-gen-null-encr* branch.

#2 - 23.10.2015 14:50 - Tobias Brunner

- Tracker changed from Issue to Bug

- Target version set to 5.3.4

#3 - 23.10.2015 16:39 - Peter Whisker

Thank you Tobias.

Regards
Peter

#4 - 09.11.2015 11:19 - Tobias Brunner

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Priority changed from High to Normal

- Resolution set to Fixed