strongSwan - Feature #3461

make default ciphers stronger

22.05.2020 17:10 - Yuri B

Status:	Closed	**Start date:**	22.05.2020
Priority:	Low	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:	5.9.0		
Resolution:	Fixed		

Description

Let's make default cipher set stronger. I remember reading about how GCM wasn't included because of old linux or something. There's no point of keeping that backward compat as those distros went EOL long ago. I don't see why a strongwan distribution on latest Fedora is requesting to use CBC instead of anything more sane available.

Thanks.

Associated revisions

Revision c7bef954 - 12.06.2020 13:45 - Tobias Brunner

proposal: Add AES-GCM to the ESP default AEAD proposal

References #3461.

Revision 33412158 - 12.06.2020 13:47 - Tobias Brunner

ike: Send AEAD ESP default proposal first

We generally prefer AEAD nowadays.

References #3461.

History

#1 - 25.05.2020 13:44 - Tobias Brunner

- Status changed from New to Feedback

- Target version set to 5.9.0

> I remember reading about how GCM wasn't included because of old linux or something.

That's generally still a problem because we can't query what algorithms the kernel actually supports. So unlike the IKE proposals, which are based on the algorithms provided by plugins, we have to guess what algorithms the kernel will support (if it doesn't support one of the negotiated algorithms, CHILD_SA installation will simply fail with a kernel error).

But I agree that AES-GCM is pretty widely available nowadays and it's listed as a MUST in RFC 8221, so I suppose we can add an AEAD default proposal for ESP that includes AES-GCM with one of the next releases.

#2 - 12.06.2020 13:48 - Tobias Brunner

- Category changed from configuration to libcharon

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to Fixed