strongSwan - Bug #2085

Charon unable to handle multiple certificates in aggressive mode

16.08.2016 18:57 - Pavel Kankovsky

Status:	Closed	**Start date:**	16.08.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	ikev1		
Target version:	5.5.1		
Affected version:	5.4.0	**Resolution:**	Fixed

Description

Commit d489e7557 modified Charon to accept multiple certificates from the other party in IKEv1 messages but the modification was restricted to the main mode and the aggressive mode remained restricted to one certificate in a message. The restriction prevented strongSwan from connecting to a certain instance of Fortinet IPsec VPN that required the aggressive mode and was sending the whole certificate chain in R1. I have removed remaining restrictions in `src/libcharon/encoding/message.c` (see the attached patch--it was made for 5.4.0 but I am sure 5.5.0 is affected as well) and it works now.

Associated revisions

Revision 22b839e6 - 17.08.2016 10:30 - Tobias Brunner

ikev1: Accept more than one certificate payload in aggressive mode

Fixes #2085.

History

#1 - 17.08.2016 10:31 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category set to ikev1

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.5.1

- Resolution set to Fixed

Thanks. Fixed with the associated commit.

Files

strongswan-5.4.0-certpayloads.patch	1.04 KB	16.08.2016	Pavel Kankovsky