strongSwan - Bug #55

Implement SHA512/384/256 HMAC with proper truncation in kernel

23.05.2008 21:37 - Martin Willi

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	Martin Willi	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	4.3.6		
Affected version:	5.9.2	**Resolution:**	

Description

Implement SHA512/384/256 HMAC with proper truncation in kernel

History

#1 - 12.06.2008 14:28 - Martin Willi

Submitted a patch, see http://kerneltrap.org/mailarchive/linux-kernel/2008/6/5/2039114. Needs more work to get it in vanilla.

#2 - 25.08.2009 14:48 - Andreas Steffen

- Target version set to 4.3.5

#3 - 17.10.2009 09:47 - Andreas Steffen

- Target version changed from 4.3.5 to 4.3.6

Assigned to 4.3.6 release

#4 - 03.12.2009 11:41 - Martin Willi

- Status changed from New to Closed

Patches accepted in net-next for 2.6.33:

http://www.mail-archive.com/linux-crypto@vger.kernel.org/msg03903.html
http://www.mail-archive.com/linux-crypto@vger.kernel.org/msg03906.html

strongSwan 4.3.6 will support SHA256/384/512 with half bits truncation. The old 96 bit truncation for SHA256 can be specified with the sha256_96 proposal keyword.