strongSwan - Bug #437

keymat_v2.c:derive_ike_keys may have mem leak

06.11.2013 07:13 - yeping xing

Status:	Closed	**Start date:**	06.11.2013
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	charon		
Target version:	5.1.2		
Affected version:	5.1.1	**Resolution:**	Fixed

Description

Hi:

In the latest version,

derive_ike_keys :
....
line 271:
if (dh->get_shared_secret(dh, &secret) != SUCCESS) {
return FALSE;
}
....
line 358:
chunk_clear(&secret);

The secret were allocted by dh->get_shared_secret,and it was freed at line 358.
But,there may be some mistakes between line 271 and line 358,and it returned FALSE
without free the secret.

Associated revisions

Revision c49c3f32 - 06.11.2013 10:24 - Tobias Brunner

ikev2: Properly free DH secret in case of errors during IKE key derivation

Fixes #437.

History

#1 - 06.11.2013 10:26 - Tobias Brunner

- Tracker changed from Issue to Bug

- Description updated

- Category set to charon

- Status changed from New to Closed

- Assignee set to Tobias Brunner

- Target version set to 5.1.2

- Resolution set to Fixed

Fixed with the associated commit. Thanks for the report.