

openQA Tests - action #89122

[sle][security][sle15sp4] fips: add some more openssl tests, dhparam and also s_server/s_client

2021-02-25 15:49 - msmeissn

Status:	New	Start date:	
Priority:	Normal	Due date:	
Assignee:	bchou	% Done:	0%
Category:	New test	Estimated time:	40.00 hours
Target version:			
Difficulty:			
Description			
We have some non working stuff in FIPS mode with openssl.			
https://bugzilla.suse.com/show_bug.cgi?id=1182764			
OPENSSL_FORCE_FIPS_MODE=1 openssl dhparam -out dhparams_2048.pem 2048 errors with:			
..			
140657399079360:error:050C90CA:Diffie-Hellman routines:DH_generate_parameters_ex:non FIPS method:crypto/dh/dh_gen.c:31:			
can you add a "openssl dhparam 2048" test to the existing fips suite?			
Also testing s_client and s_server in FIPS mode with DHE and potentially others.			
openssl s_server -key generatedkey -cert generatedcert -dhparam dhparams_2048.pem -cipher DHE			
and then connect to localhost:4433 e.g. with			
openssl s_client -connect localhost:4443			

History

#1 - 2021-03-04 07:52 - tjyrinki_suse

- Subject changed from fips: add some more openssl tests, dhparam and also s_server/s_client to [sle][security] fips: add some more openssl tests, dhparam and also s_server/s_client

- Start date deleted (2021-02-25)

#2 - 2021-04-28 08:23 - llzhao

- Subject changed from [sle][security] fips: add some more openssl tests, dhparam and also s_server/s_client to [sle][security][sle15sp4] fips: add some more openssl tests, dhparam and also s_server/s_client

- Category set to New test

- Assignee set to bchou

- Estimated time set to 40.00 h