Keywords	Commit ID	Comments	TD	Files changed	Commit i - 1	
hack, hacky, hackery						
	007c80eae4e1f36e28a9645c485c14ec61baed4e	This is a hacked version of files.pl for systems that can't do a 'make files'.	N			
	753585b94897f5628cf9c13d8a6c97861074febb	hack to add version info on MSVC	N			
	2e52e7df518d80188c865ea3f7bb3526d14b0c08	A hack to make Visual C++ 5.0 work correctly when linking as a DLL using /MT.	N			
	ec59112a822e16a539bc5dd1b8bed12afbcb82b8	- * 18-Mar-1997 - eay - A quick hack :-) version 1.1, it would probably help to save or load the private key :-)This is a hack required because s_ssl and c_ssl are sharing the same BIO structure and SSL_set_bio() and SSL_free() - * automatically BIO_free non NULL entries.	N			
	7f458a48ff3a231d5841466525d2aacbcd4f6b77	../../include/openssl/symhacks.h ../../include/openssl/rsa.h	?			
	6928b6171ada6d0de5a024a188dc7a68094d2dca	my @ssl_symbols = &do_defs("LIBSSL", $ssl, $symhacks); my @crypto_symbols = &do_defs("LIBCRYPTO", $crypto, $symhacks);	?			
	9e58d1192da2dbd6544f73f73362db6ae9f2c045	Ugly hack here, because PPC assembler syntax seem to vary too much from platforms to platform	Y			
	f578075a93c7418f72ba000d1225cb0d9fd7df5d	If a test fails, try with defining the logical name OPENSSL_NO_ASM (yes, -it's an ugly hack!) and rebuild. A VMSINSTALlable version (way in the future, unless someone else hacks). -- shareable images (DLL for you Windows folks).	N			
	0f53f939a10ad9eeee555dc235936e515118f216	Also remove the old symbol hacks. They were needed needed to shorten some names to 31 characters, and to resolve other symbol clashes. Because we now compile with /NAMES=(AS_IS,SHORTENED), this is no longer required.	Y			
	e84193e43dbd3da23845ef9fcfcb5e364049a396	This is a horrible hack, but is needed because recursive inclusion of files in different directories does not work well with HP C. The "[]" hack is because in .OPT files, each line inherits the previous line's file spec as default, so if no directory spec is present in the current line and the previous line has one that doesn't apply, you're in for a surprise.	Y			
	0dc225577c402f71b1aa3b533193ed645f4fe19b	The B<-prexit> option is a bit of a hack. We should really report information whenever a session is renegotiated.Deleted	N			
	169394d45645bb686a187db6517aab7caeae82b0	The B<-prexit> option is a bit of a hack. We should really report +information whenever a session is renegotiated.		/doc/apps/s_client.pod.orig		
	28a0841bf58e3813b2e07ad22f19484308e2f70a	* It's imperative that these macros get defined before openssl/bio.h gets * included. Otherwise, the AI_PASSIVE hack will not work properly. * For clarity, we check for internal/cryptlib.h since it's a common header * that also includes bio.h.	Y	crypto/bio/bio_lcl.h		
	9fe2bb77c40f5fd3624b30f1b0c3cd8b791ca615	SCRIPTS=myhack	?			
	7d130f68fc429609df9fd2ddec3218306d66206e	Hack cflags for better warnings (dev option) #######################	?			
	8ff2af548303d311ce3591406111f77862875a60	Gnomovision' (which makes passes at compilers) written by James Hacker.	N			
	a8eda4312db1f98cffda38670e2d40d36566785a	Hacks to shorten symbols to 31 characters or less, or OpenVMS. This mimics - * what's done in symhacks.h, but since this is a very local header file, I - * prefered to put this hack directly here. -- Richard Levitte. Deleted the hack and the FILE	**Y**	engines/ccgost/gost_lcl.h	c64879d3f3cc4c7f1c436a9fe3bd109847a23629	228
	d10dac1187fbb12fdb44a0386f1619b79b40d264	/include/openssl/symhacks.h . File containing these lines was deleted	N			
	ff4b7fafb315df5f8374e9b50c302460e068f188	Just links to ../include/openssl/symhacks.h	?			
	2bec39eb86986349d2538fffc821f2e1106cee14	Just links to ../include/openssl/symhacks.h	?			
	21fa90b242b2078bfee324188227de8d02376e68	Just links to ../include/openssl/symhacks.h . File containing these lines was deleted	N			
	ebd8df0ed8a2f39a63662a5246df9e00e240efec	Just links to ../include/openssl/symhacks.h	?			
	bbd86bf5424a611cb6b77a3a17fc522931c4dcb8	Just links to ../include/openssl/symhacks.h	?			
	170b735820ac6a3857733fccf889cde9d723ddc8	../include/openssl/symhacks.h	?			
	d9b8b89bec4480de3a10bdaf9425db371c19145b	/* We use a temporary STACK so we can chop and hack at it */. The piece of code following it was removed	Y	crypto/x509/x509_vfy.c		343
	5378186199eec800e0508c5ac1c3545d072b8c31	../include/openssl/symhacks.h	?			
	3b089ca21b782f66083a11dbb51ba7279a4c2187	../include/openssl/symhacks.h	?			
	7644a9aef8932ed4d1c3f25ed776c997702982be	../../include/openssl/symhacks.h	?			
	2ab9687479c10c4c4ebfdfcf6d068fe581bd44e4	../include/openssl/symhacks.h	?			
	ba67253db19d0319f672d47aa359032e5e66d1b8	../../include/openssl/symhacks.h	?			
	bd989745b7a4796dceff89d93b6b7ac1561c6227	../../include/openssl/symhacks.h	?			
	3c4e064e784fc96e937d99dba58df2e761d5ba7c	../include/openssl/symhacks.h	?			
	1eb97c3ecd5a9c7faa9436d506735be0bd7c3b4b	../../include/openssl/symhacks.h	?			
	f84f31fc36e1e4e0e647661b8ac410ee97ce77ce	../../include/openssl/symhacks.h. File was deleted	N			
	bd3602eb8948dcd3a03cb56fbfa80bb4ac569cdb	../../include/openssl/symhacks.h	?			
	d3bcab845e3cae7e97500c9ae5d380ff16f1fedc	. File was deleted	N			
	168e8374eeb7ae50816efcac23f65e7e1294360a	../../include/openssl/symhacks.h	?			
	768c53e1b615023b7eb4b2b5df2f0ab5fc3f4af8	../../include/openssl/symhacks.h	?			
	7f572e958b13041056f377a62d3219633cfb1e8a	../../include/openssl/symhacks.h	?			
	9cc6fa1ce83ce7857660ee11c3285651ceff0f43	../../include/openssl/symhacks.h	?			
	b83fb854da7ab6b61c3ec62372cfb857987107fd	../../include/openssl/symhacks.h	?			
	c742f56e94176d4274bb31e796e9ea9eb084f60f	../../include/openssl/symhacks.h	?			
	7240557b7d6a06cd7e4cd50e52fb1e62d0a750e0	../../include/openssl/symhacks.h	?			

	4f70d04593951905fa560719ae7aaa032aca14ca	../../include/openssl/symhacks.h	?			
	252d6d3aa62dccf0dc826644b7da0b6bafa3831b	../../include/openssl/symhacks.h	?			
	7070e5ca2fa41940d56599bf016a45cb1c0e03f0	../../include/openssl/symhacks.h	?			
	9ec1e03194568630a2e58232d56e9d37dd13ed7d	../../include/openssl/symhacks.h	?			
	501083049590455b1862edd7573fd51bb37bb037	../../include/openssl/symhacks.h	?			
	07bbc92ccb96d48044220d2ed2cf818323baeb26	../../include/openssl/symhacks.h	?			
	a14e9ff713cbe7dbbba2aa667466490291cffc68	../../include/openssl/symhacks.h	?			
	a3667c316ae60ef454fb804221c3ca44af30a9aa	../../include/openssl/symhacks.h	?			
	bf1605518a085256320ff4a36054445f842d5c1c	../../include/openssl/symhacks.h	?			
	699f1635242d509d0e47ca3132d1b5682a6a32b7	../../include/openssl/symhacks.h	?			
	b0700d2c8de79252ba605748a075cf2e5d670da1	Removed 18-Apr-96 tjh Original hacking ; links to ../../include/openssl/symhacks.h; static double OpenSSL_MSVC5_hack = 0.0; OpenSSL_MSVC5_hack = (double)name[0] * (double)name[1];	?			
	075c8795857de6746ee662e50ebe44055a494f51	/* EVIL HACK! */ was removed	**Y**	apps/s_server.c	7	
	8ba708e5166b02ab61f2762d36b3e7b7455e9c06	Some servers hang if client hello > 256 bytes as hack workaround - * chop number of supported ciphers to keep it well below this if we - * use TLS v1.2 . Link to ../include/openssl/symhacks.h	?			
	b9908bf9b8d6d609736b537f4ecda720ff5dc078	Some servers hang if client hello > 256 bytes as hack workaround + * chop number of supported ciphers to keep it well below this if we + * use TLS v1.2 + */	?			
	f8e0a5573820bd7318782d4954c6643ff7e58102	../../include/openssl/symhacks.h	?			
	0e56b4b42439d0842956a6730dec904ed70bbef7	/* + * We have to set the BIO's to NULL otherwise they will be free()ed + * twice. Once when th s_ssl is SSL_free()ed and again when c_ssl is + * SSL_free()ed. This is a hack required because s_ssl and c_ssl are + * sharing the same BIO structure and SSL_set_bio() and SSL_free() + * automatically BIO_free non NULL entries. You should not normally do + * this or be required to do this + */	Y	demos/threads/mttest.c		
	2f1a5d1694c4b59ea94115ed4e9577c5bb826c26	../../include/openssl/symhacks.h	?			
	dad0b512e649336440e2b3cc9d667c56d9a91eff	/* - * We have to set the BIO's to NULL otherwise they will be free()ed - * twice. Once when th s_ssl is SSL_free()ed and again when c_ssl is - * SSL_free()ed. This is a hack required because s_ssl and c_ssl are - * sharing the same BIO structure and SSL_set_bio() and SSL_free() - * automatically BIO_free non NULL entries. You should not normally do - * this or be required to do this - */ crypto/threads/mttest.c was deleted	**Y**	crypto/threads/mttest.c	8cbb048c3ea41 6f2bd8a3706d02 7f3aa26ef08d9	1071
	15db6a40d3569789329d3f6f84e47e0e0e8f9caa	../../include/openssl/symhacks.h	?			
	8b7080b0b7f30669c0784d8aa73388f95bbd056b	-/* Compatibility hack, the dynamic library uses this form in the path */ -static const char *engine_4758_cca_id_alt = "4758_cca"; The file engines/e_4758cca.c was deleted	**Y**	engines/e_4758cca.c	f51e5ed6b4b91d 12228da873db7 2aa28109d1797	937
	3149baf83cb703f060b1e6eeb440a45e010a626b	../../include/openssl/symhacks.h	?			
	2ff00bdbc4aad268e07df82541ff4a16b1f91fe8	../../include/openssl/symhacks.h	?			
	75f648aa06933a5b5436d2ae4a764be68ab22c4d	../../include/openssl/symhacks.h	?			
	984d6c6052169bcae8010de33f7796e455536d61	../../include/openssl/symhacks.h	?			
	156561b0ade98b22df0e3ebc63682e54129c2cb4	static double SSLeay_MSVC5_hack = 0.0. The line was removed	?			
	1c9c243509d017244764545dc01e40d962423bbb	* If first argument is a colon, skip it. Because in "interactive" - * mode our prompt is a colon and we can cut/paste whole lines - * by doing this hack. The line was deleted	**Y**	apps/openssl.c		12
	8bbda94c6e25a24cf842f3c4df9fcfa6b4606ce2	../../include/openssl/symhacks.h	?			
	1e898fb0f58c9b6cee13917a8453809b1009fec2	../../include/openssl/symhacks.h	?			
	8011f64efbad435efb1c77e9ac38b4d216091c96	../../include/openssl/symhacks.h	?			
	df2ee0e27d2db02660c1d15fe6a3e38be9df0a60	../../include/openssl/symhacks.h	?			
	f5098edb14ce7da8db814dd392358d53c2b81496	Sometimes, the functions in L<OpenSSL::Test> are quite tedious for some +repetitive tasks. This module provides functions to make life easier. +You could call them hacks if you wish.	?			
	64b25758edca688a30f02c260262150f7ad0bc7d	../../include/openssl/symhacks.h	?			
	231efb936548320e81c3259b41c26bb71e83720a	../../include/openssl/symhacks.h	?			
	3a3cb629d9ef66639198f6130f58e30f0606adc8	../../include/openssl/symhacks.h	?			
	ade44dcb16141c8a30ca6c56a1fd1a0b14dcc360	../../include/openssl/symhacks.h	?			
	6142f5c640f98429d4798b8418e8cc2cf6cc1fb8	../../include/openssl/symhacks.h	?			
	2d5d70b15559f9813054ddb11b30b816daf62ebe	../../include/openssl/symhacks.h	?			
	6fc2ef20a92a318aa5aacf9c907fa70df98f6a41	../../include/openssl/symhacks.h	?			
	7e729bb5a3ff1b940061045d1f83b7fc01d32b4b	../../include/openssl/symhacks.h	?			
	3b848c642cdbca17c686c95b8fd655e5b1f5df2a	../../include/openssl/symhacks.h	?			

	7e5363abe3c00d9db037f464f3c121e194bb5bb6	../../include/openssl/symhacks.h	?			
	0bc2f365558ed5980ce87d6b2704ca8649ca2a4a	../../include/openssl/symhacks.h	?			
	040b93353e8b48cfc0e2429d96eb3a27f259512d	../../include/openssl/symhacks.h	?			
	593e9c638c58e1a510c519db0d024527113330f3	../../include/openssl/symhacks.h	?			
	74924dcb3802640d7e2ae2e80ca6515d0a53de7a	../../include/openssl/symhacks.h	?			
	f2e19cb15e3d68c748ce3dc2b791be9a2fc14fd3	../../include/openssl/symhacks.h	?			
	3a752c85ee38a92d7777b8fe1cce2e54bf619529	../../include/openssl/symhacks.h	?			
this is wrong	99d63d4662e16afbeff49f29b48f1c87d5558ed0	This is wrong but Netscape -and MSIE do this as do many certificates. So although this is incorrect -it is more likely to display the majority of certificates correctly.(What's a pod file)	N	doc/man1/x509.pod		
	b0ac0a8ef832b2753c9ace2a79bcf875c87d8c88	/* XXX: surely this is wrong - if ret is 0, it just didn't verify; Just a semi-colon was added	N			
	bd4e152791acc2a41441bd5713cbddc4b3645d27	This is wrong but Netscape +and MSIE do this as do many certificates. So although this is incorrect +it is more likely to display the majority of certificates correctly.	N	doc/apps/x509.pod		
	db1842132fc4e87cdc006757fbc27dc1c1562337	id_function does not need to be defined under Windows NT or 95, the +correct function will be called if it is not. Under unix, getpid() +is call if the id_callback is not defined, for solaris this is wrong +(since threads id's are not pid's) but under IRIX it is correct +(threads are just processes sharing the data segement).	N	doc/ssleay.txt		
workaround for bug	78c990c156ba79521e98728e9a604b4c5cc8adec	# Workaround for bug in RAND des2 test output */. 2) Workaround for old broken DES3 MCT format which added bogus - # extra lines: after [ENCRYPT] or [DECRYPT] skip until first - # COUNT line. The file was deleted	**Y**	fips/fipsalgtest.pl	00b4ee7664051a0dc589b1d81ba56582576a6ca4	1209
	2b4b28dc32ce7623f6169b43cd18585174de6b20	# Workaround for bug in RAND des2 test output */	Y	fips/fipsalgtest.pl		
temporary solution						
something bad is going on						
this indicates a more fundamental problem						
something serious is wrong						
doubt that this would work						
risk of this blowing up						
remove this code	c87386a2cd586368a61d86ede03319f910d050f4	TODO(TLS1.3): This is temporary, because TLSv1.3 resumption is completely + * different. For now though we're still using the old resumption logic, so + * to avoid test failures we need this. Remove this code!	Y	ssl/ssl_sess.c		
remove me	619d8336d00fe19bc694e61e772b5838d7e422e5	/* TODO(TLS1.3) REMOVE ME: Version indicator for draft -18 */	Y	include/openssl/tls1.h		
	b5b253b1bfe55d0d1be4c45dafed8d789ab97c17	/* TODO(TLS1.3) REMOVE ME: Version indicator for draft -17 */	Y	include/openssl/tls1.h		
	49ae742398aecd81551d59f421e4116a5b8a4ea9	/* TODO: This is temporary - remove me */. This comment and the line following it was removed	**Y**	ssl/statem.c	--	18
	f8e0a5573820bd7318782d4954c6643ff7e58102	/* TODO: This is temporary - remove me */	Y	ssl/statem.c		
remove me before production						
it doesn't work yet						
doesn't work yet						
Fix later						
revise later						
redo later	78c990c156ba79521e98728e9a604b4c5cc8adec	See if we have a comma separated list of parameters if so copy rest of line back to buffer and redo later. The file was deleted.	?	fips/aes/fips_gcmtest.c		
	b5dd1787401256f6a4d70686debf13b096f2bc22	See if we have a comma separated list of parameters if so copy rest of line back to buffer and redo later. Added this line.	?			
reframe later						
redesign later						

save for later							
Fix in the future							
revise in the future							
save for the future							
redo in the future							
reframe in the future							
redesign in the future							
is problematic	99d63d4662e16afbeff49f29b48f1c87d5558ed0	If B<cert> is set to NULL all possible recipients are tried. This case however is problematic.	?				
	ef75444d0873ab4b35070b6362867b7b712515e6	The combination of perl and sed takes advantage of their respective - # capabilities. Some sed implementations aren't greedy (enough), which - # is problematic with the some regexps. However, the sed d command is - # simply easier in sed. This comment was removed	?				
	bb26842d1c8f99c1267b45361a2fc76822c0f913	en't greedy (enough), which - # is problematic with the some regexps. However, the sed d command is - # simply easier in sed. This comment was removed	?	Configurations/unix-Makefile.tmpl			
	f4e175e4afe900bce8624882c42d25056fd74188	Performance is [incredible for a 32-bit processor] 1.76 cycles per processed byte. Comparison to compiler-generated code is problematic,because results were observed to vary from 2.1 to 7.6 cpb depending on compiler's ability to inline small functions.	N				
	64f9f40696f993406e53c16d7c9d815004afd8ad	We can't shutdown properly if we are in the middle of a - * handshake. Doing so is problematic because the peer may send a - * CCS before it acts on our close_notify. The comment was removed	N				
	7bb196a71adef8440b6152b6174651a9c25588f1	We can't shutdown properly if we are in the middle of a - * handshake. Doing so is problematic because the peer may send a - * CCS before it acts on our close_notify.	N				
	5f8e9a477a18551052f2019c1f374061acbaa5e6	If B<cert> is set to NULL all possible recipients are tried. This case however is problematic.	?				
	b7e46a9bce052d2d5b134bdfe0b5e34c90e000d6	SHA1 is in widespread use in certificates but it only offers 80 bits -of security. This is problematic as anything above level 1 will reject -them. The comment was removed.	N				
	0f817d3b2705f315f4c8c22b5dfee0218848f37a	SHA1 is in widespread use in certificates but it only offers 80 bits +of security. This is problematic as anything above level 1 will reject +them.	?				
	4407700c40f766cedccc26479d18ff2e8bc19ff4	SHA1 is in widespread use in certificates but it only offers 80 bits +of security. This is problematic as anything above level 1 will reject +them.	?				
	cb3b9b132336d7931c047a95a0d7638b8e470e55	Fair comparison +# with vendor compiler is problematic, because OpenSSL doesn't define +# BN_LLONG [presumably] for historical reasons, which drives compiler +# toward 4 times 16x16=32-bit multiplicatons [plus complementary +# shifts and additions] instead.	N				
	386828d02913b26918ac2883623e3f66103a120d	This option is to allow + use of the new ASN1 code on platforms where exporting structures + is problematical (for example in shared libraries) but exporting + functions returning pointers to structures is not	N				
causes issue							
cause for issue							
this can be a mess							
this is temporary and will go away							
hope everything will work							
workaround	2b4b28dc32ce7623f6169b43cd18585174de6b20	# Workaround for bug in RAND des2 test output */	Y	fips/fipsalgtest.pl			
	417a24dba560ce1419b75d0f8cf5ded819b31f31	Chil ENGINE unload workaround	N				
	5814d829e612b4daab2a2d1a9f1e6979f9c56d32	Workaround for slow RAND_poll() on some WIN32 versions. in NEWS file	N				
	47e0a1c335295d7548ecd1860954ee4f988d9804	On some versions of WIN32 Heap32Next is very slow. This can cause + excessive delays in the RAND_poll(): over a minute. As a workaround + include a time check in the inner Heap32Next loop too. (Comment in CHANGES file)	N				
	2712a2f6256a69e914b174e1915b029b1f4b9554	/* Workaround for broken implementations that use signature + * algorithm OID instead of digest. + */	Y	crypto/cms/cms_lib.c			

	6c17629f914aaf17979e96fb0abd8af20ea9d1fc	THe B<X509_V_FLAG_X509_STRICT> flag disables workarounds for some broken +certificates and makes the verification strictly apply B<X509> rules.	?			
	e30dd20c0ec57b96c31aa3ffea9f646aa32368ba	WARNING: applications which + included workarounds for the old buggy behaviour will need to be modified + or they could free up already freed BIOs. Applications which +included workarounds for this bug (e.g. freeing BIOs more than once) should +be modified to handle this fix or they may free up an already freed BIO.	?			
	e5fa864f62c096536d700d977a5eb924ad293304	Disable workarounds for broken certificates which have to be disabled +for strict X.509 compliance.	?			
	837f2fc7a4a8073b269538b7d0168c0cd7edd951	Special case as client bug workaround: the previously used cipher may + * not be in the current list, the client instead might be trying to + * continue using a cipher that before wasn't chosen due to server + * preferences	Y	ssl/s3_srvr.c		
	2aa2a5775f7f4c008f958141c1e05c1c9bcdd135	CAPI_trace(ctx, "Enumerate bug: using workaround\n");	?			
	7a18ecb2df34baa6de462bfcf9379e38209d224b	CAPI_trace(ctx, "Enumerate bug: using workaround\n");	?			
	5cda6c458211c2b5803f9616b192fd2e8c1c47f3	This bug workaround has been + * around since SSLeay so hopefully it is either fixed + * now or no buggy implementation supports compression	Y	ssl/t1_enc.c		
	65613f23bafeb26145b86b2649d0f554411bb052	There are few cases documented in PROBLEMS file, +consult it for possible workaround before you beat the drum.	N			
	cd27b13b1dec5fc9998374a76eb82c7163fb6f05	The workaround may be to change the following lines in apps/Makefile and +test/Makefile:	N			
	ce074604c410397ef22085eaf026e73d98b2b721	Fortunately there is workaround, +hire /bin/ksh to do the job /bin/sh fails to do. The comment is in PROBLEMS file	N			
	4c3a2d64e43901ae954d4e6382ac7995330c6dc0	I'm not committing - corresponding workaround into the HEAD as Makefile.shared - reportedly needs even more work... The comment was removed	N			
	2757c67da2c68d8757cf4314993f7b46f5a351f5	I'm not committing + corresponding workaround into the HEAD as Makefile.shared + reportedly needs even more work... The comment is in ChangeLog.0_9_7-stable_not-in-head file	N			
	bc501570109e7837e1de1689de1eec9420e4cf89	Disable workarounds for broken certificates	Y	crypto/x509/x509_vfy.h		
	a32fc687dedf6d4368dc0fc18320654191c16bb8	Adding this +option enables various workarounds.	?			
	beab098d5385850baa600d5788b2b8549f962c5e	Workaround for some broken clients that put the signature + * OID instead of the digest OID in digest_alg->algorithm	Y	crypto/pkcs7/pk7_doit.c		
	d745af4b0cc5d37ffa662aa04dcbfb2855c0f034	workaround for the SECG curve names secp192r1 + * and secp256r1 (which are the same as the curves + * prime192v1 and prime256v1 defined in X9.62)	?			
	52e5e5c2baf15c1f8fcec2cd7ecd21a39a8011dc	Workaround: modify the target to +O2 when building with no-asm.	N			
	76a03d568e9592d41cc0b8b2ced16dc612bff130	There might +or might not be a workaround.	N			
	623e9e66c0de2981420af35c9f06b2c900538d22	echo "As a workaround, we'll use a bundled old copy of pod2man.pl." >&2	?			
	80e1495b99ac6a614137db595e420b013c76554a	The workaround may be to change the following lines in apps/Makefile.ssl and +test/Makefile.ssl:	N			
	c21506ba024adb6d5655a92d61c1d3824e5dedcf	Disable SSL 3.0/TLS 1.0 CBC vulnerability workaround that was added + * in OpenSSL 0.9.6d. Usually (depending on the application protocol) + * the workaround is not needed. SSL_OP_ALL: various bug workarounds that should be rather harmless. + * This used to be 0x000FFFFFL before 0.9.7.	Y	ssl/ssl.h		
	2962243d19ec76c66fee5a551a6d26946716c364	echo "As a workaround, we'll use a bundled old copy of pod2man.pl." >&2	?			
	381a146dc6e4c35e06546926fe7c48328aeb103d	Change bctest to avoid here-documents inside command substitution + (workaround for FreeBSD /bin/sh bug. The comment is in CHANGES file	N			
	51008ffce12b1bf6077efccc19623d9f811a9a8c	It is safe and recommended to use B<SSL_OP_ALL> to enable the bug workaround	?	/doc/ssl/SSL_CTX_set_options.pod		
	36026dfc0103b289b53b1ae9307cfd634b97afae	W.r.t. (b) + such data would previously have always leaked in application code and + workarounds were in place to make the memory debugging turn a blind eye + to it.	N			
	f2ab7d13921890e40c847fba3d22c936a2681f6b	It is safe and recommended to use SSL_OP_ALL to enable the bug workaround	?	doc/ssl/SSL_CTX_set_options.pod		
	06da6e49777285f50aeb1b920d950a9bd27fef52	Move SSL_OP_TLS_ROLLBACK_BUG out of the SSL_OP_ALL list of recommended + bug workarounds. The comment is in CHANGES file	N			
	884e26080f494634728bfb599245d414f2787067	Change bctest to avoid here-documents inside command substitution + (workaround for FreeBSD /bin/sh bug). The comment is in CHANGES file	N			
	1266eefdb66db6c01e859ae672ccc19261e75bbf	Add padding to workaround bugs in F5 terminators. Existing Line.	N			
	ab83e31414286ccdc35fbacf976f64a910a6c718	Add padding to workaround bugs in F5 terminators.	?			

	99d63d4662e16afbeff49f29b48f1c87d5558ed0	The B<X509_V_FLAG_X509_STRICT> flag disables workarounds for some broken +certificates and makes the verification strictly apply B<X509> rules. Adding this +option enables various workarounds. For strict X.509 compliance, disable non-compliant workarounds for broken +certificates. The actual checks done are rather +complex and include various hacks and workarounds to handle broken +certificates and software. Applications which +included workarounds for this bug (e.g. freeing BIOs more than once) should +be modified to handle this fix or they may free up an already freed BIO. B<Bugs>: enable various bug workarounds. Same as B<SSL_OP_ALL>. Adds a padding extension to ensure the ClientHello size is never between +256 and 511 bytes in length. This is needed as a workaround for some +implementations.It is usually safe to use B<SSL_OP_ALL> to enable the bug workaround +options if compatibility with somewhat broken implementations is +desired.The B<X509_V_FLAG_X509_STRICT> flag disables workarounds for some broken +certificates and makes the verification strictly apply B<X509> rules.	?	doc/man3/X509_VERIFY_PARAM_set_flags.pod		
	2c7b4dbc1af9cfae4e4afd7c4a07db95a1133a6a	Some servers hang if client hello > 256 bytes as hack workaround + * chop number of supported ciphers to keep it well below this if we + * use TLS v1.2	Y	statem/statem_clnt.c		
	e8fd2a4cb49c91e5af1608b3cd494e2a8cf02ae2	We have no replacement for Perl's canonpath(), so the best workaround + for now is to rename the OpenSSL source directory, as follows (please + adjust for the actual source directory name you have)	?	NOTES.VMS		
	0907d7105cbf8d72b267f4453f96dd636fa59621	unsigned char workaround_good	?			
	5b8fa431ae8eb5a18ba913494119e394230d4b70	workaround_good = constant_time_eq_8(rsa_decrypt[padding_len], + (unsigned)(s->version >> 8));	?			
	fcd9c8c0149d989bf0ab28e14bbaa49e5060db9b	The easiest workaround is to force struct addrinfo to be the + * 64-bit variant when compiling in P64 mode.	Y	crypto/bio/bio_lcl.h		
	23d38992fca13773291ca647220707bfb0636361	/* - * workaround for ultrix cc: without 'case 0', the optimizer does - * the switch table by doing a=top&3; a--; goto jump_table[a]; - * which fails for top== 0 - */ The comment wasremoved from the file crypto/bn/bn_lib.c	**Y**	crypto/bn/bn_lib.c		5
	6ab364149d8b76b5d2341a2e708e727cad060416	The workaround may be to change the following lines in apps/Makefile and -test/Makefile. Fortunately there is workaround, -hire /bin/ksh to do the job /bin/sh fails to do. The comments were removed from a file.	N			
	f4a748a17d6a38f410acd342e8539d0e7196cbdb	Generate CFLAGS as an array of individual characters. This is a + * workaround for the situation where CFLAGS gets too long for a C90 string + * literal + */	Y	util/mkbuildinf.pl		
	0dc225577c402f71b1aa3b533193ed645f4fe19b	Adding this -option enables various workarounds. The comment was removed from the file.	?			
	169394d45645bb686a187db6517aab7caeae82b0	Adding this +option enables various workarounds.	?	doc/apps/s_server.pod.orig		
	8ff2af548303d311ce3591406111f77862875a60	The best choice is to find some unambiguous delimiter +strings that you can use in your template instead of curly braces, and +then use the C<DELIMITERS> option. However, if you can't do this for +some reason, there are two easy workarounds	Y	external/perl/Text-Template-1.46 /lib/Text/Template.pm		
	8ba708e5166b02ab61f2762d36b3e7b7455e9c06	* Some servers hang if client hello > 256 bytes as hack workaround - * chop number of supported ciphers to keep it well below this if we - * use TLS v1.2 - */ Comment removed from ssl/s3_srvr.c . Comment Some servers hang if client hello > 256 bytes as hack workaround + * chop number of supported ciphers to keep it well below this if we + * use TLS v1.2*/ added to	Y	ssl/statem/statem_clnt.c. ssl/s3_srvr.c(R)		
	b9908bf9b8d6d609736b537f4ecda720ff5dc078	Some servers hang if client hello > 256 bytes as hack workaround - * chop number of supported ciphers to keep it well below this if we - * use TLS v1.2 was removed from ssl/s3_clnt.c . Comment Some servers hang if client hello > 256 bytes as hack workaround + * chop number of supported ciphers to keep it well below this if we + * use TLS v1.2 added to ssl/s3_clnt.c	Y	ssl/s3_clnt.c		
	b3e2272c59a5720467045e2ae62940fdb708ce76	Special case as client bug workaround: the previously used - * cipher may not be in the current list, the client instead - * might be trying to continue using a cipher that before wasn't - * chosen due to server preferences. We'll have to reject the - * connection if the cipher is not enabled, though. Comment removed from ssl/s3_srvr.c	**Y**	ssl/s3_srvr.c	2ff00bdbc4aad268e07df82541ff4a16b1f91fe8	248
	4f46473a86c9e3741203b22d4d401a3763583494	There might -or might not be a workaround. For more -details and workarounds see: <URL: http://rt.openssl.org/Ticket/Display.html?user=guest&pass=guest&id=2771>	N			

	a8e4ac6a2fe67c19672ecf0c6aeafa15801ce3a5	Remove SSL_OP_TLS_BLOCK_PADDING_BUG This is a workaround so old that nobody remembers what buggy clients it was for. It's also been broken in stable branches for two years and nobody noticed (see https://boringssl-review.googlesource.com/#/c/1694/). The comment This bug - * workaround has been around since SSLeay so hopefully it is either - * fixed now or no buggy implementation supports compression [steve] was removd from	**Y**	ssl/record/ssl3_record.c		22
	a3680c8f9c33d4190c367572645980ccdb9d5bbf	The comment * Some servers hang if client hello > 256 bytes as hack workaround - * chop number of supported ciphers to keep it well below this if we - * use TLS v1.2 - */ was removed from ssl/s23_clnt.c[DF]	**Y**	ssl/s23_clnt.c	13c9bb3ecec5f8 47b4c5295249e 039d386e2d10e	594
	32ec41539b5b23bc42503589fcc5be65d648d1f5	* Special case as client bug workaround: the previously used - * cipher may not be in the current list, the client instead - * might be trying to continue using a cipher that before wasn't - * chosen due to server preferences. We'll have to reject the - * connection if the cipher is not enabled, though. Comment removed from ssl/s3_srvr.c . The same comment added to ssl/s3_srvr.c	Y	ssl/s3_srvr.c		
	186bb90705f848806783de512b3df6872552b304	The B<X509_V_FLAG_X509_STRICT> flag disables workarounds for some broken	N	doc/crypto/X509_VERIFY_PARAM_set_flags.pod		
	7e1b7485706c2b11091b5fa897fe496a2faa56cc	BIO_printf(bio_err, - " -bugs - Switch on all SSL implementation bug workarounds\n"); Removed from apps/s_client.c	?			
	dee502be89e78e2979e3bd1d7724cf79daa6ef61	/* mips-sgi-irix6.5-gcc vv -mabi=64 bug workaround */ the comment was removed from crypto/bf/bftest.c	**Y**	crypto/bf/bftest.c	30cd4ff294252c 4b6a4b69cbef6a 5b4117705d22	537
	02a36fdae8cb503e2f88eac52eb3053431089397	This bug + * workaround has been around since SSLeay so hopefully it is either + * fixed now or no buggy implementation supports compression [steve]. The same cooment was removed from ssl/s3_cbc.c	Y	ssl/record/ssl3_record.c **ssl/s3_cbc.c**		220
	367eab2f9f1d1131356118507d21534558863365	Chil ENGINE unload workaround.	N			
	bdc234f3c362b211d9e9384da93f8a0ff212787e	Disable code workaround for ancient and obsolete Netscape browsers - and servers: an attacker can use it in a ciphersuite downgrade attack.	N			
	97a0cc52812c6cc075ec7da849dd496f0e6cf5a4	DMD32_XARRAY triggers workaround for compiler bug we ran into in -# 32-bit message digests. The same comment was added too to some file	N			
	7a4dadc3a6a487db92619622b820eb4f7be512c9	" -hack - workaround for early Netscape code\n");	?			
	f09e7ca94bd428203da770a874604754dace1b02	DMD32_XARRAY triggers workaround for compiler bug we ran into in +# 32-bit message digests. The same comment was removed from some other file.	N			
	9e9858d1cf28e39cfd214b5c508188d5016728fd	Workaround is now obsolete */ was removed from ssl/s3_clnt.c	**Y**	ssl/s3_clnt.c		24
	0f113f3ee4d629ef9a4a30911b22b224772085e5	workaround for the SECG curve names secp192r1 - * and secp256r1 (which are the same as the curves - * prime192v1 and prime256v1 defined in X9.62) was removd from apps/ecparam.c . The same comment was added to apps/ecparam.c . The comment "As a workaround we timeout the select every - * second and check for any keypress. In a proper Windows - * application we wouldn't do this because it is inefficient." was removed from apps/s_server.c . The comment " Under DOS (non-djgpp) and Windows we can't select on stdin: + * only on sockets. As a workaround we timeout the select every + * second and check for any keypress. In a proper Windows + * application we wouldn't do this because it is inefficient." was added to apps/s_server.c. The comment "/* mips-sgi-irix6.5-gcc vv -mabi=64 bug workaround */" was removed from crypto/bf/bftest.c . The same comment was added to /crypto/bf/bftest.c . The comment workaround for ultrix cc: without 'case 0', the optimizer does - * the switch table by doing a=top&3; a--; goto jump_table[a]; - * which fails for top== 0 was removed from crypto/bn/bn_lib.c . The same comment was added to crypto/bn/bn_lib.c . The comment "ultrix cc workaround, see comments in bn_expand_internal" was removed from crypto/bn/bn_lib.c . The same comment was added to the same file . The comment "/* Disable workarounds for broken certificates */" was added to crypto/x509/x509_vfy.h . /* Some servers hang if client hello > 256 bytes - * as hack workaround chop number of supported ciphers - * to keep it well below this if we use TLS v1.2 - */ was removed from ssl/s23_clnt.c . The same comment was added to ssl/s23_clnt.c. The comment "if compression is in operation the first packet may not be of - * even length so the padding bug check cannot be performed. This bug - * workaround has been around since SSLeay so hopefully it is either - * fixed now or no buggy implementation supports compression [steve] - */ " was removed from ssl/s3_cbc.c. The same comment was added to ssl/s3_cbc.c . The comment "Some servers hang if client hello > 256 bytes - * as hack workaround chop number of supported ciphers - * to keep it well below this if we use TLS v1.2" was removed and added to ssl/s3_clnt.c . The comment "Special case as client bug workaround: the previously used cipher may - * not be in the current list, the client instead might be trying to - * continue using a cipher that before wasn't chosen due to server - * preferences. We'll have to reject the connection if the cipher is not - * enabled, though. */" was removed from ssl/s3_srvr.c and later added to the same file.	Y	apps/ecparam.c apps/s_server.c crypto/bf/bftest.c crypto/bn/bn_lib.c crypto/x509/x509_vfy.h ssl/s23_clnt.c ssl/s3_cbc.c ssl/s3_srvr.c		

	68d39f3ce6ff4f65170d94f7310b3f485f33328d	workaround for ultrix cc: without 'case 0', the optimizer does + * the switch table by doing a=top&3; a--; goto jump_table[a]; + * which fails for top== 0 was added to crypto/bn/bn_lib.c. Somme +,- in the same file.	Y	crypto/bn/bn_lib.c		
	dbd87ffc210328eb8670c24a427318172c1e334d	/* workaround for ultrix cc: without 'case 0', the optimizer does - * the switch table by doing a=top&3; a--; goto jump_table[a]; - * which fails for top== 0 */ was removed and later added to crypto/bn/bn_lib.c	Y	crypto/bn/bn_lib.c		
	488f16e31b8f5ec2513410929325d0830d76762d	Generate CFLAGS as an array of individual characters. This is a + * workaround for the situation where CFLAGS gets too long for a C90 string + * literal added to /util/mkbuildinf.pl	Y	/util/mkbuildinf.pl		
	a4a934119dd213e16c9d8b11150a4815604c13bb	echo "As a workaround, we'll use a bundled old copy of pod2man.pl." >&2	N			
	78c990c156ba79521e98728e9a604b4c5cc8adec	Workaround for old broken DES3 MCT format which added bogus - # extra lines: after [ENCRYPT] or [DECRYPT] skip until first - # COUNT line. and " Workaround for bug in RAND des2 test output */" was removed from fips/fipsalgtest.pl[DF]	**Y**	fips/fipsalgtest.pl	00b4ee7664051a0dc589b1d81ba56582576a6ca4	1209
	45f55f6a5bdcec411ef08a6f8aae41d5d3d234ad	The comment /* Some servers hang if client hello > 256 bytes - * as hack workaround chop number of supported ciphers - * to keep it well below this if we use TLS v1.2 - */ was removed from and added to ssl/s23_clnt.c	Y	ssl/s23_clnt.c		
	455b65dfab0de51c9f67b3c909311770f2b3f801	workaround_mask will be 0xff if version_good is - * non-zero (i.e. the version match failed). Otherwise - * it'll be 0x00.	?			
	76b10e13c22681d09567192583c81b296aed279e	There are few cases documented in PROBLEMS file, -consult it for possible workaround before you beat the drum.	N			
	bcd3e36c467f00833a5aefa45e9fcb304bf052f0	Same as above				
	14e961921a7ff21c90ef944b33ada2658bca6255	As a workaround use the maximum pemitted + encrypted premaster secret. As a workaround use the maximum permitted	N			
	38c654819c520b43f6b2f9d3240a969aa78a876c	Workaround for the "TLS hang bug" (see FAQ and PR#2771): if the - TLS client Hello record length value would otherwise be > 255 and - less that 512 pad with a dummy extension containing zeroes so it - is at least 512 bytes long.	N			
	ee724df75d9ad67fd954253ac514fddb46f1e3c6	BIO_printf(bio_err," -hack - workaround for early Netscape code\n");	?			
	2866441a9027b0f7f07c675ba450eff897e16a91	For strict X.509 compliance, disable non-compliant workarounds for broken -certificates.	N			
	01f2f18f3c7e229bd4b1b2e3e150722175c64971	Adds a padding extension to ensure the ClientHello size is never between +256 and 511 bytes in length. This is needed as a workaround for some +implementations. The comment is in pod file				
	86f6e8669c02e9077fa0dd1883f64b61328599a1	Add TLS padding extension workaround for broken servers.	N			
	3a98f9cf20c6af604799ee079bec496b296bb5cc	Workaround for some implementation that use a signature OID *	Y	crypto/rsa/rsa_ameth.c		
	4fcdd66fff5fea0cfa1055c6680a76a4303f28a2	Add padding to workaround bugs in F5 terminators. Experimental workaround TLS filler (WTF) extension. Based on a suggested - workaround for the "TLS hang bug" (see FAQ and PR#2771): if the TLS client - Hello record length value would otherwise be > 255 and less that 512 - pad with a dummy extension containing zeroes so it is at least 512 bytes - long.	N			
	0467ea68624450ecece4cde0d5803499aaff19c2	Experimental workaround TLS filler (WTF) extension. Based on a suggested + workaround for the "TLS hang bug" (see FAQ and PR#2771): if the TLS client + Hello record length value would otherwise be > 255 and less that 512 + pad with a dummy extension containing zeroes so it is at least 512 bytes + long.	N			
	4dc836773e042806235bd724acc711f0cb9b049b	" encrypted premaster secret. As a workaround use the maximum pemitted" was removed and added to CHANGES file	N			
	5ef24a806d0c74920fbfbb930c40f460a62688bd	For more +details and workarounds see: + + <URL: http://rt.openssl.org/Ticket/Display.html?user=guest&pass=guest&id=2771>	N			
	3d7bf77f6183d3971d40aa1a906809eb8628ac2b	encrypted premaster secret. As a workaround use the maximum permitted - and + in CHANGED file	N			
	adb46dbc6dd7347750df2468c93e8c34bcb93a4b	/* workaround_mask will be 0xff if version_good is + * non-zero (i.e. the version match failed). Otherwise + * it'll be 0x00.	?			
	a693ead6dc75455f7f5bbbd631b3a0e7ee457965	/* NB: if compression is in operation the first packet may not be of + * even length so the padding bug check cannot be performed. This bug + * workaround has been around since SSLeay so hopefully it is either + * fixed now or no buggy implementation supports compression [steve] + */	Y	ssl/s3_cbc.c		
	2acc020b770920657a169bf6be4ff12b254255e6	Above comment was removed from ssl/t1_enc.c	**Y**	ssl/t1_enc.c		76
	3a778a2913bede0d537abbcebe8093d3d7b1aa8a	"Disable workarounds for broken certificates which have to be disabled -for strict X.509 compliance." was removed and "For strict X.509 compliance, disable non-compliant workarounds for broken +certificates." were added to doc/apps/verify.pod	N			
	13cfb043439c8e4b5b96cec42003a8d15e9387fd	Various bug workarounds are set, same as setting B<SSL_OP_ALL> was added and removed from ssl/SSL_CONF_cmd.pod	N			

	c7b7984ac914d33590dfe9e46e35336f5e4f723f	B<Bugs>: enable various bug workarounds. Same as B<SSL_OP_ALL>. was added and removed from a pod file	N				
	3db935a9e5e62fcbde719b2a03ce8941bb13514a	B<Bugs> enable various bug workarounds. Same as B<SSL_OP_ALL>. in doc/ssl/SSL_CONF_cmd.pod	N				
	41409651be9bdbd5296979e7bca273c8faefc9ef	The comment /* The Rhapsody 5.5 (a.k.a. MacOS X) compiler bug - * workaround. <appro@fy.chalmers.se> */ was removed from ssl/s2_clnt.c	**Y**	ssl/s2_clnt.c			5
	579d553464604832911c1eb08d014f487e54e0ff	Workarounds for some servers that hang on long client hellos.in NEWS file	N				
	800e1cd969f5c89f142857f63416b44ab063fb1b	/* Some servers hang if client hello > 256 bytes + * as hack workaround chop number of supported ciphers + * to keep it well below this if we use TLS v1.2 + */ was added to ssl/s23_clnt.c and ssl/s3_clnt.c	Y	ssl/s23_clnt.c ssl/s3_clnt.c			
	f4e1169341ad1217e670387db5b0c12d680f95f4	As a workaround use the maximum pemitted + client version in client hello, this should keep such servers happy + and still work with previous versions of OpenSSL.in CHANGES file	N				
	288fe07a6e3e4d61e71db84ce31135cc6d1789ce	Workaround for old broken DES3 MCT format which added bogus + # extra lines: after [ENCRYPT] or [DECRYPT] skip until first + # COUNT line.	Y	fips/fipsalgtest.pl			
	c415adc26ffd07c7a9f42e7ec3aff0b404a4ce5f	Disable code workaround for ancient and obsolete Netscape browsers + and servers: an attacker can use it in a ciphersuite downgrade attack. + Thanks to Martin Rex for discovering this bug. in CHANGES file	N				
	88f2a4cf9ced521e2c2874a1c32af0eeaa027f40	Same as above	N				
can cause problems	99d63d4662e16afbeff49f29b48f1c87d5558ed0	"The use of an in-memory text database can cause problems when large -numbers of certificates are present because, as the name implies -the database has to be kept in memory. " was removed from doc/apps/ca.pod file and 2) " This can cause problems if you need characters that aren't available in -PrintableStrings and you don't want to or can't use BMPStrings." was removed from the doc/apps/req.pod file 3) This can cause problems as the -time_t value can overflow on some systems resulting in unexpected results. was removed from doc/crypto/ASN1_TIME_set. pod file . The removed lines were added to different pod files	N				
	77a795e4b0ac541b305561811bab355f5bb316fd	The use of an in-memory text database can cause problems when large was - and added to doc/apps/ca.pod file	N				
	5eb8f71204626843a5ff1e7016d5d9e5a9598ee8	Explicitly de-initing can cause problems (e.g. where a library that uses + OpenSSL de-inits, but an application is still using it). in CHANGES file	N				
	a724e79ed761ea535a6c7457c90da5ff4b1cea69	This can cause problems as the +time_t value can overflow on some systems resulting in unexpected results. +New applications should use ASN1_TIME_adj() instead and pass the offset value +in the B<offset_sec> and B<offset_day> parameters instead of directly +manipulating a time_t value. in doc/crypto/ASN1_TIME_set.pod file	N				

	24956ca00f014a917fb181a8abc39b349f3f316f	SIGUSR1/SIGUSR2 are no longer mapped in the read tty stuff because it - can cause problems. in crypto/des/VERSION file	N			
	684400ce192dac51df3d3e92b61830a6ef90be3e	Although no details of the signed portion of the certificate can be changed this can cause problems with some applications: e.g. those using the certificate fingerprint for blacklists. in CHANGES file	N			
	deb2c1a1c58fb738b3216b663212572170de8183	On some platforms, this casting can cause problems. was removed from crypto/rijndael/README file	N			
	3ab56511120b7a67ed4e4dbac9d60e5d1520a453	On some platforms, this casting can cause problems. was added to crypto/rijndael/README file	N			
	dd46d58f65bd3a342bbcd8586680942be643fc7d	The use of an in memory text database can cause problems when large +numbers of certificates are present because, as the name implies +the database has to be kept in memory. in doc/apps/ca.pod file 2) +This can cause problems if you need characters that aren't available in +PrintableStrings and you don't want to or can't use BMPStrings. in doc/apps/req.pod file 3) These comments were removed from some other files.	N			
	aba3e65f2c8b02e6c458681db56dc1594266cba9	The use of an in memory text database can cause problems when large +numbers of certificates are present because, as the name implies +the database has to be kept in memory. in /doc/man/ca.pod file 2) This can cause problems if you need characters that aren't available in +PrintableStrings and you don't want to or can't use BMPStrings. in doc/man/req.pod file	N			
	4b55c2a3a9590fd27f865e2325195a2e14215bce	These are defined in wincrypt.h and can cause problems */ was removed frome_os.h	**Y**	e_os.h		3
	f5eac85edcb6e8b24593282c9e140daeeb758cac	/* These are defined in wincrypt.h and can cause problems */ was added to e_os.h file	Y	e_os.h		
	58964a492275ca9a59a0cd9c8155cb2491b4b909	Defining SIGACTION causes sigaction() to be used instead of signal(). + SIGUSR1/SIGUSR2 are no longer mapped in the read tty stuff because it + can cause problems. in crypto/des/VERSION file	N			
may cause problems	34216c04229ffaa564adb204cea87bc6b5ed4fb1	Repeat of may cause problem	N			
this is temporary	71728dd8aa3acc0bc9d621f8c4a4032aa3325fe4	This is temporary code while we do not have support for + # TLS1.3 resumption.	Y	test/ssl-tests/protocol_version.pm		
	c87386a2cd586368a61d86ede03319f910d050f4	TODO(TLS1.3): This is temporary, because TLSv1.3 resumption is completely + * different. For now though we're still using the old resumption logic, so + * to avoid test failures we need this. Remove this code!	Y	ssl/ssl_sess.c		
	49ae742398aecd81551d59f421e4116a5b8a4ea9	/* TODO: This is temporary - remove me */ . The comment was removed	**Y**	ssl/statem.c		18
	f8e0a5573820bd7318782d4954c6643ff7e58102	/* TODO: This is temporary - remove me */	Y	ssl/statem.c		
in the future	08e588b7d5cefbfd107c88416900165a28a5b59e	Number of seconds in the future that an SCT timestamp can be, by default, -// without being considered invalid. was removed and added	N			
	c22aa33e29ce162c672c9b2f0df591db977d4e9b	Number of seconds in the future that an SCT timestamp can be, by default, +// without being considered invalid. was added 2) timestamp is in the future". By default, this will be set to the -current time (obtained by calling time()) if possible. was removed and added	N			
	e25233d99c30885bdf97bfb6df657e13ca2bf1da	timestamp is in the future". Typically, the time provided to this function will -be the current time. was removed and added	N			
	1871a5aa8a538c2b8ac3d302c1e9e72867f5ee0f	1) The timestamp of the SCT will be compared to this, to check that it was not - * issued in the future. RFC6962 states that "TLS clients MUST reject SCTs whose - * timestamp is in the future", so SCT verification will fail in this case. was removed 2) If the SCT's timestamp is after this time, it will be interpreted as + * having been issued in the future. RFC6962 states that "TLS clients MUST + * reject SCTs whose timestamp is in the future", so an SCT will not validate + * in this case. was added 3)supposedly issued in the future. RFC6962 states that "TLS clients MUST reject -SCTs whose timestamp is in the future". was removed 4) issued in the future. RFC6962 states that "TLS clients MUST reject SCTs whose +timestamp is in the future". Typically, the time provided to this function will +be the current time. was added 5) The timestamps of the SCTs will be compared to this, to check that they were - * not issued in the future. was removed 6)If an SCT's timestamp is after this time, it will be interpreted as having + * been issued in the future. was added	N			
	1fa9ffd934429f140edcfbaf76d2f32cc21e449b	1) The timestamp of the SCT will be compared to this, to check that it was not + * issued in the future. RFC6962 states that "TLS clients MUST reject SCTs whose + * timestamp is in the future", so SCT verification will fail in this case. was added 2) If the SCT's signature is incorrect, its timestamp is in the future (relative to +the time in CT_POLICY_EVAL_CTX), or if it is otherwise invalid, the validation +status will be SCT_VALIDATION_STATUS_INVALID. was added 3) The time returned by SSL_SESSION_get_time() will be used to evaluate whether any +presented SCTs have timestamps that are in the future (and therefore invalid). was added 4) Gets the time, in milliseconds since the Unix epoch, that will be used as the + * current time when checking whether an SCT was issued in the future. + * Such SCTs will fail validation, as required by RFC6962. was added 5) The timestamps of the SCTs will be compared to this, to check that they were + * not issued in the future. RFC6962 states that "TLS clients MUST reject SCTs + * whose timestamp is in the future", so an SCT will not validate in this case. was added	N			
	ac9fc67a488427bc3e987f5a4c235e8fbeedf711	In test 1 we set + * the record sequence number to be way off in the future. This should not + * have an impact on the record replay protection because the record should + * be dropped before it is marked as arrived	N			

	69853045e1154236d440eba363a001033f5e3781	WARNING : below extension types are *NOT* IETF assigned, and could - * conflict if these types are reassigned and handled specially by OpenSSL - * in the future was removed from test/ssltest.c[DF] and added to test/ssltest_old.c[NF]	Y	test/ssltest.c[DF] test/ssltest_old.c[NF]	ababe86b9674dca24ffb6b342fe7af852cf53466	
	2ad9ef06a6aadeeb78a05ce18ace0ea5f300401b	Except for "(unknown)", the + actual value is currently ignored but may + be used in the future. was added to README file	N			
	71a04cfca03bf6d5a93ad3ffd23e0fb9e0da2919	Also, dynamic locks are currently not used internally by OpenSSL, but -may do so in the future. was removed	N			
	f578075a93c7418f72ba000d1225cb0d9fd7df5d	A VMSINSTALlable version (way in the future, unless someone else hacks). was removed	N			
	0f53f939a10ad9eeee555dc235936e515118f216	A VMSINSTALlable version (way in the future, unless someone else hacks). was removed 2)The Architecture Is Alpha, IA64 or whatever comes in the future. was removed from multiple places	N			
	9fe2bb77c40f5fd3624b30f1b0c3cd8b791ca615	"mk1mf" and "unixmake". Others may appear - in the future. was removed	N			
	88087414def54cd55dfebc172f17f79ed7d3034a	Currently recognised build schemes are + "mk1mf" and "unixmake". Others may appear + in the future. was added	N			
	46bf69b5934d45f9e00b962f26cf15b8fe8a1e56	As per - April 2005 Platform SDK is equipped with Win64 compilers, as well - as assemblers, but it might change in the future. was removed	N			
	8ba708e5166b02ab61f2762d36b3e7b7455e9c06	Discard the message if sequence number was already there, is too far - * in the future, already in the queue or if we received a FINISHED - * before the SERVER_HELLO, which then must be a stale retransmit. was removed and added	N			
	d9b3554b2d9724bc2d1621a026ddaf0223e2d191	Note, it could be easy to inherit from the "gnu" style... however, +;; one never knows if that style will change somewhere in the future, +;; so I've chosen to copy the "gnu" style values explicitely instead +;; and mark them with a comment. was added	N			
	a1accbb1d704da9a25b18e7053ee191a8f510d93	For now we just deal with this as a block of data. In the future we will + #want to parse this was added	?			
	631c1206334adfb21758220362a56fa157a47596	#For now we just deal with this as a block of data. In the future we will + #want to parse this was added	?			
	dee502be89e78e2979e3bd1d7724cf79daa6ef61	WARNING : below extension types are *NOT* IETF assigned, and could - * conflict if these types are reassigned and handled specially by OpenSSL - * in the future was removed from ssl/ssltest.c[DF] and added to test/ssltest.c[NF]	Y	ssl/ssltest.c[DF] test/ssltest.c[NF]	30cd4ff294252c4b6a4b69cbef6a5b4117705d22	
	1711f8de45cdee01fdf21e55db5522d23b450867	/* XXX: this is a possible improvement in the future */ was removed from ssl/record/d1_pkt.c[DF] and added to ssl/record/rec_layer_d1.c	Y	ssl/record/d1_pkt.c[DF] ssl/record/rec_layer_d1.c	9e7ba3b2a2ffc049b4b5c664cf33473b475ce323	
	999005e49355d738a017fa300630864f832b6273	/* XXX: this is a possible improvement in the future */ was removed from ssl/d1_pkt.c[DF] and added to ssl/record/d1_pkt.c [NF]	Y	ssl/d1_pkt.c[DF] ssl/record/d1_pkt.c[NF]	c103c7e266145dc922115a2c3079776bb8216939	
	24956ca00f014a917fb181a8abc39b349f3f316f	The Architecture Is Alpha, IA64 or whatever comes in the future. was removed	N			
	39a24e8889be8b7a63afdb6f999e4314e2b94671	I may in the future include a perl script that does this code - removal automatically for those in the USA :-). was removed 2)At this point in time only read and write conditions can be -used but in the future I can see the situation for other -conditions, specifically with SSL there could be a condition -of a X509 certificate lookup taking place and so the non- -blocking BIO_read would require a retry when the certificate -lookup subsystem has finished it's lookup. was removed 3) RC4 that has no blocking and so the function will not write - anything into 'out', it would still be a good idea to pass a - variable for 'out' that can hold 8 bytes just in case the cipher is - changed some time in the future. was removed 4) I have lots more references etc, and will update this list in the future, -30 Aug 1996 - eay was removed 5)This is now a bit dated, quite a few of the SSL_ functions could be -SSL_CTX_ functions. I will update this in the future. 30 Aug 1996 was removed from doc/ssleay.txt[DF]	N			
	0f113f3ee4d629ef9a4a30911b22b224772085e5	Check thisUpdate is valid and not more than nsec in the future was removed and added. 2) Discard the message if sequence number was already there, is - * too far in the future, already in the queue or if we received - * a FINISHED before the SERVER_HELLO, which then must be a stale - * retransmit. was removed and added. 3) WARNING : below extension types are *NOT* IETF assigned, and could + * conflict if these types are reassigned and handled specially by OpenSSL + * in the future was removed and added	Y	ssl/ssltest.c		
	03b637a730e4a298c360cc143de7564060c06324	There are thoughts to allow proxy certificates with a line in the -default openssl.cnf, but that's still in the future. was removed from doc/HOWTO/proxy_certificates.txt .	N			
	9cd50f738ff55eae2a64f872492d3a7ce115f18d	/* WARNING : below extension types are *NOT* IETF assigned, and + could conflict if these types are reassigned and handled + specially by OpenSSL in the future */ was added in ssl/ssltest.c file	Y	ssl/ssltest.c		
	36df342f9b2faeeecc70a279395e9433f35e4622	alternative tweak calculation algorithm is based on suggestions + # by Shay Gueron. psrad doesn't conflict with AES-NI instructions + # and should help in the future... was added in crypto/aes/asm/aesni-x86_64.pl	N			
	ed28aef8b455be436f252dfceac49a958a92e53b	VIA promises CPUs that won't require alignment in the future. was removed engines/e_padlock.c . 2) They promise to - improve it in the future, but for now we can just as well - pretend that it can only handle aligned input... */ was removed from engines/e_padlock.c	N			

	d5dfa7cd82804eec165569deeb4181d60c08b0f6	The Architecture Is Alpha, IA64 or whatever comes in the future. was removed from test/maketests.com	N			
	58f41a926a73bd5c49beb91991b486d4e0b544f5	too far in the future or the fragment is already in the queue */ was removed and added to ssl/d1_both.c	N			
	481547f0feff816dfee963b518761a9d66d84ea9	/* Discard the message if sequence number was already there, is + * too far in the future or the fragment is already in the queue */ was added to ssl/d1_both.c	N			
	cc8cc9a3a175690d146a209d648652bbd53b3e68	The Architecture Is Alpha, IA64 or whatever comes in the future. was added in multiple files	N			
	00b4e083fddd5c4bdaae342f28839e27319c5ada	VIA promises CPUs that won't require alignment in the future. - For now padlock_aes_align_required is initialized to 1 and - the condition is never met... */ - /* C7 core is capable to manage unaligned input in non-ECB[!] - mode, but performance penalties appear to be approximately - same as for software alignment below or ~3x. They promise to - improve it in the future, but for now we can just as well - pretend that it can only handle aligned input... */ were removed and added in engines/e_padlock.c	N			
	6c06918ede75af1967a113e44336d1bfef50fa19	C7 core is capable to manage unaligned input in non-ECB[!] + mode, but performance penalties appear to be approximately + same as for software alignment below or ~3x. They promise to + improve it in the future, but for now we can just as well + pretend that it can only handle aligned input...	N			
	1875e6db29fb832d3cac101024ccb1f690b35028	As per + April 2005 Platform SDK is equipped with Win64 compilers, as well + as assemblers, but it might change in the future.	N			
	36d16f8ee0845d932e250286e8e236580470e35b	/* XXX: this is a possible improvement in the future */	Y	ssl/d1_pkt.c		
	d9bfe4f97cd4244beb0598cc348d68b04dac7068	There are thoughts to allow proxy certificates with a line in the +default openssl.cnf, but that's still in the future.	N			
	7d15a556f85d103e2d2a91b19de8e1898d4842e0	VIA promises CPUs that won't require alignment in the future.	N			
	4083a229b45df718b7b52994962c5d1ac62b2c8b	/* XXXX This may be fixed in the future */ was removed from ssl/ssl_cert.c	**Y**	ssl/ssl_cert.c		109
	95f8c7195c13dfdeab64b99044e33af44ef37b79	The variant 64-bit processors cause concern should GCC support explicit schedulers + # for these chips in the future.	N			
	c2e4f17c1a0d4d5115c6ede9492de1615fe392ac	Some + time in the future, des_old.h and the libdes compatibility functions + will be completely removed.	N			
	f185e725a00a76cee0bcd0a3beb92a257d2b6325	The net effect needs to be that at any - time, it is deterministic to know whether an ENGINE is in use or - can be safely removed (or unloaded in the case of the other type - of reference) without invalidating function pointers that may or - may not be used indavertently in the future.	N			
	f196522159a514915e6d749a71febd08e7a09b71	/* Check thisUpdate is valid and not more than nsec in the future */	N			
	bc36ee6227517edae802bcb0da68d4f04fe1fb5e	/* XXXX This may be fixed in the future */ was removed and added	Y	apps/app_rand.c		
	5270e7025e11b2fd1a5bdf8d81feded1167b1c87	The net effect needs to be that at any + time, it is deterministic to know whether an ENGINE is in use or + can be safely removed (or unloaded in the case of the other type + of reference) without invalidating function pointers that may or + may not be used indavertently in the future.	N			
	3b211619224a6d1b3a777fab9aefe742fa845cbb	Also, dynamic locks are currently not used internally by OpenSSL, but +may do so in the future.	N			
	8c197cc55eda97fba9c51254fd0e1da7259ab174	A VMSINSTALlable version (way in the future, unless someone else hacks).	N			
	58dc480ffd18007960569db728b93bab499d5deb	A VMSINSTALlable version (way in the future, unless someone else hacks). was removed and added	N			
	f7fd2ff72e88f49468a388b9806aceb4f1eacd29	A VMSINSTALlable version (way in the future, unless someone else hacks).	N			
	7d7d2cbcb02206f3393681f2bce198e11e2e185b	/* XXXX This may be fixed in the future */ was added to	Y	ssl/ssl_cert.c		
	8073036dd62848b616c6a817c155c3255074ec83	removed obsolete files (the test scripts will be replaced + by better Test::Harness variants in the future)	N			
	db1842132fc4e87cdc006757fbc27dc1c1562337	At this point in time only read and write conditions can be -used but in the future I can see the situation for other -conditions, specifically with SSL there could be a condition -of a X509 certificate lookup taking place and so the non- -blocking BIO_read would require a retry when the certificate -lookup subsystem has finished it's lookup. was removed . 2) Please remember that even if you are using ciphers like - RC4 that has no blocking and so the function will not write - anything into 'out', it would still be a good idea to pass a - variable for 'out' that can hold 8 bytes just in case the cipher is - changed some time in the future. was removed 3) I have lots more references etc, and will update this list in the future, -30 Aug 1996 - eay was removed . 1) and 2) were alseo added to ssome files	N			
	651d0aff98d28e2db146afa1790e9e22f3ef22db	I may in the future include a perl script that does this code + removal automatically for those in the USA :-). was removed and added.	N			

	d02b48c63a58ea4367a0e905979f140b7d090f86	I may in the future include a perl script that does this code + removal automatically for those in the USA :-). was added . 2)At this point in time only read and write conditions can be +used but in the future I can see the situation for other +conditions, specifically with SSL there could be a condition +of a X509 certificate lookup taking place and so the non- +blocking BIO_read would require a retry when the certificate +lookup subsystem has finished it's lookup. was added 3) Please remember that even if you are using ciphers like + RC4 that has no blocking and so the function will not write + anything into 'out', it would still be a good idea to pass a + variable for 'out' that can hold 8 bytes just in case the cipher is + changed some time in the future. was added. 4) I have lots more references etc, and will update this list in the future, +30 Aug 1996 - eay was added . 5) /* else data is still being written out, we will get written + * some time in the future */ was added.	N			
will go away	dee502be89e78e2979e3bd1d7724cf79daa6ef61	This includes evil casts to remove const: they will go away when full ASN1 + * constification is done.	Y	include/openssl/asn1t.h		
	0f113f3ee4d629ef9a4a30911b22b224772085e5	This includes evil casts to remove const: they will go away when full ASN1 + * constification is done.	Y	crypto/asn1/asn1t.h		
	524289baa514dbaa457c15af59f70d0669b9528f	HACK to disable operation if no OPENSSL_FIPSSYMS option. -# will go away when tested more fully. The comment was removed from util/fipsas.pl	**Y**	util/fipsas.pl		4
	5d439d69552e753debc48461293517b66b0b94b4	HACK to disable operation if no OPENSSL_FIPSSYMS option. +# will go away when tested more fully.	Y	util/fipsas.pl		
	9d6b1ce6441c7cc6aed344f02d9f676ab5e04217	This includes evil casts to remove const: they will go away when full + * ASN1 constification is done.	Y	crypto/asn1/asn1t.h		
	2fdf5d7c2354b76bcc429b5f2c582a580e12d50d	This function will insert callbacks so that -the SSLeay libraries will use the same malloc(), free() and realloc() as -your application so 'problem 3)' mentioned above will go away. The comment was removed	N			
	651d0aff98d28e2db146afa1790e9e22f3ef22db	For Windows 95/NT, add CRYPTO_malloc_init() to your program before any +calls to the SSLeay libraries. This function will insert callbacks so that +the SSLeay libraries will use the same malloc(), free() and realloc() as +your application so 'problem 3)' mentioned above will go away. The comment is not in a source code file	N			
	d02b48c63a58ea4367a0e905979f140b7d090f86	This function will insert callbacks so that +the SSLeay libraries will use the same malloc(), free() and realloc() as +your application so 'problem 3)' mentioned above will go away. The comment is in a non-source code file.	N			
TYPE 1						
this isn't very solid						
don't use this	2e52e7df518d80188c865ea3f7bb3526d14b0c08	/* Don't use this structure directly. */ was removed	?			
	71a04cfca03bf6d5a93ad3ffd23e0fb9e0da2919	/* Don't use this structure directly. */ was removed	?			
	865b55ac8e32e9815d20b55fb05e66b61558cf6d	/* Don't use this with d2i_ASN1_BOOLEAN() */ was removed	N			
	dee502be89e78e2979e3bd1d7724cf79daa6ef61	-/* Don't use this with d2i_ASN1_BOOLEAN() */ was removed. 2) /* Don't use this structure directly. */ These comments were removed and added back to some files	?			
	24956ca00f014a917fb181a8abc39b349f3f316f	-cbc3_enc.c - des_3cbc_encrypt() source, don't use this function. was removed	?			
	39a24e8889be8b7a63afdb6f999e4314e2b94671	-2nd note: I'm note quite sure whether the gawk script really handles all -possible inputs for the request right! Today I don't use this construction -anymore myself. was removed	N			
	86d21d0b9577322ac5da0114c5fac16eb49b4cef	/* Wolfgang Marczy <WMarczy@topcall.co.at> reports that - * the RegQueryValueEx call below can hang on NT4.0 (SP6). - * So we don't use this at all for now. */	N			
	ceea4bf047abf369debf5c312928331f107400c6	Let's just say, *I* - * don't use this in a mission-critical environment, so it would be stupid for - * anyone to assume that it is solid and/or tested enough when even its author - * doesn't place that much trust in it.	N			
	4c3296960de32e5abfbb8f4703a2ce624d82669f	/* Don't use this structure directly. */ was added	N			
	2c45bf2bc9be4704c63b024d5721c1f537adb0f2	/* Don't use this with d2i_ASN1_BOOLEAN() */ was added	N			
	6e32d0a74be5fc9340c66dd03f11f89f8ac193bf	-cbc3_enc.c - des_3cbc_encrypt() source, don't use this function. was removed and added to some file	?			
	cc85ec447b65509070a50414664d62d397701df9	/* Wolfgang Marczy <WMarczy@topcall.co.at> reports that + * the RegQueryValueEx call below can hang on NT4.0 (SP6). + * So we don't use this at all for now. */	N			
	d1855cc7af56acb62407618711ee5e90a805e231	Let's just say, *I* + * don't use this in a mission-critical environment, so it would be stupid for + * anyone to assume that it is solid and/or tested enough when even its author + * doesn't place that much trust in it. You have been warned.	N			
	db1842132fc4e87cdc006757fbc27dc1c1562337	2nd note: I'm note quite sure wether the gawk script really handles all -possible inputs for the request right! Today I don't use this construction -anymore myself. was removed and added to some files	N			
	dfeab0689f69c0b4bd3480ffd37a9cacc2f17d9c	/* Don't use this with d2i_ASN1_BOOLEAN() */ was added	N			

	d02b48c63a58ea4367a0e905979f140b7d090f86	cbc3_enc.c - des_3cbc_encrypt() source, don't use this function. was added. 2) 2nd note: I'm note quite sure wether the gawk script really handles all +possible inputs for the request right! Today I don't use this construction +anymore myself.	?			
get rid of this	865b55ac8e32e9815d20b55fb05e66b61558cf6d	BIG UGLY WARNING! This is so damn ugly I wanna puke. Unfortunately, some - * macros that use ASN1_const_CTX still insist on writing in the input - * stream. ARGH! ARGH! ARGH! Let's get rid of this macro package. Please? -- - * Richard Levitte was removed from include/openssl/asn1_mac.h [DF]	**Y**	include/openssl/asn1_mac.h		579
	dee502be89e78e2979e3bd1d7724cf79daa6ef61	/* - * BIG UGLY WARNING! This is so damn ugly I wanna puke. Unfortunately, some - * macros that use ASN1_const_CTX still insist on writing in the input - * stream. ARGH! ARGH! ARGH! Let's get rid of this macro package. Please? -- - * Richard Levitte - */ was removed from crypto/asn1/asn1_mac.h[DF] and added to include/openssl/asn1_mac.h	Y	crypto/asn1/asn1_mac.h include/openssl/asn1_mac.h	30cd4ff294252c 4b6a4b69cbef6a 5b4117705d22	579
	0f113f3ee4d629ef9a4a30911b22b224772085e5	/* BIG UGLY WARNING! This is so damn ugly I wanna puke. Unfortunately, - some macros that use ASN1_const_CTX still insist on writing in the input - stream. ARGH! ARGH! ARGH! Let's get rid of this macro package. - Please? -- Richard Levitte */ was removed from crypto/asn1/asn1_mac.h and added to crypto/asn1/asn1_mac.h	Y	crypto/asn1/asn1_mac.h		
	875a644a9047e96dfcce27af876d30460759805e	/* BIG UGLY WARNING! This is so damn ugly I wanna puke. Unfortunately, + some macros that use ASN1_const_CTX still insist on writing in the input + stream. ARGH! ARGH! ARGH! Let's get rid of this macro package. + Please? -- Richard Levitte */ was added to the file.	Y	crypto/asn1/asn1_mac.h		
just abandon it						
fix this crap						
it doesn't work yet						
crap	b6453a68bbb34c901a2eaf24012d0a3afcbf52ff	scrapped, because a) they were not interchangeable with other 32-bit	N			
	6c5b6cb035666d46495ccbe4a4f3d5e3a659cd40	We have now cleared all the crap off the end of the line	N			
	6e3d015363ed09c4eff5c02ad41153387ffdf5af	/* a miss or crap from the other end */ was removed	N			
	7ead0c89185c46378e3ed85c0012d083f4b3039b	originally there were 32-bit hpux-parisc2-* targets. They were +# scrapped, because a) they were not interchangable with other 32-bit +# targets; a) when critical 32-bit assembly modules detect if they +# are executed on PA-RISC 2.0 and thus adequate performance is +# provided.in .conf file	N			
	39a24e8889be8b7a63afdb6f999e4314e2b94671	The spelling and grammar are crap but -it is better than nothing :-) 2) Now all the above mentioned ciphers and digests libraries support high -speed, minimal 'crap in the way' type interfaces. were removed	N			
	0f113f3ee4d629ef9a4a30911b22b224772085e5	We have now cleared all the crap off the end of the - * line was removed and added to multiple files. 2)/* FIXME: setting this via a completely different prototype - seems like a crap idea */ was removed from ssl/bio_ssl.c and added to the same file	Y	ssl/bio_ssl.c		
	7b3ba508af5c86afe43e28174aa3c53a0a24f4d9	/* a miss or crap from the other end */ was removed and added	N			
	20c04a13e6af0bc7c8e1d0a94f35260593329b80	There is quite a bit of extra crap in RC4_loop() for this	?			
	c9fb4e2c8d2eabe732e1d1aabd9706d55980a4a4	/* If the state fails, put some crap in anyway */ was removed	**Y**	crypto/rand/randfile.c		3
	e7716b7a197d551a22dfdb4df6021db8e92bae5d	It appears some "scrapbook" uses of BN_CTX result in BIGNUMs being - * left in an inconsistent state when they are released (eg. BN_div). - * These can trip us up when they get reused, so the safest fix is to - * make sure the BIGNUMs are made sane when the context usage is - * releasing them.	N			
	5f747c7f4bfb7dc97179a1bbe746e083ca38d1e3	It appears some "scrapbook" uses of BN_CTX result in BIGNUMs being + * left in an inconsistent state when they are released (eg. BN_div). + * These can trip us up when they get reused, so the safest fix is to + * make sure the BIGNUMs are made sane when the context usage is + * releasing them. */	N			
	45d87a1ffe45b668cb6a6645bdc3e21a69324a41	/* FIXME: setting this via a completely different prototype + seems like a crap idea */ was added	Y	ssl/bio_ssl.c		
	175b0942ec7e82f86831916d325922817872e657	We have now cleared all the crap off the end of the + * line */	N			
	db1842132fc4e87cdc006757fbc27dc1c1562337	-Now all the above mentioned ciphers and digests libraries support high -speed, minimal 'crap in the way' type interfaces. was removed and added	N			
	651d0aff98d28e2db146afa1790e9e22f3ef22db	The spelling and grammar are crap but +it is better than nothing :-) was removed and added	N			
	58964a492275ca9a59a0cd9c8155cb2491b4b909	There is quite a bit of extra crap in RC4_loop() for this + # first round was added 2) /* a miss or crap from the other end */	?			

	d02b48c63a58ea4367a0e905979f140b7d090f86	The spelling and grammar are crap but +it is better than nothing :-) was added 2) /* We have now cleared all the crap off the end of the + * line */ 3) /* If the state fails, put some crap in anyway */ was added(TD) in crypto/rand/randfile.c	Y	crypto/rand/randfile.c		
inconsistency	2e52e7df518d80188c865ea3f7bb3526d14b0c08	error "Inconsistency between crypto.h and cryptlib.c" was removed	N			
	8ba708e5166b02ab61f2762d36b3e7b7455e9c06	Inconsistency alert: cert_chain does include the peer's certificate, - * which we don't include in s3_srvr.c 2) Inconsistency alert: cert_chain does *not* include the peer's own - * certificate, while we do include it in s3_clnt.c were removed 3) Inconsistency alert: cert_chain does include the peer's certificate, + * which we don't include in s3_srvr.c was added 4) Inconsistency alert: cert_chain does *not* include the peer's own + * certificate, while we do include it in s3_clnt.c was added	?			
	0f113f3ee4d629ef9a4a30911b22b224772085e5	# error "Inconsistency between crypto.h and cryptlib.c" - /* Inconsistency alert: cert_chain does include the peer's + * Inconsistency alert: cert_chain does include the peer's certificate, - /* Inconsistency alert: cert_chain does *not* include the + * Inconsistency alert: cert_chain does *not* include the peer's own	?			
	0ecfd920e592c4299b8154e675b164ded8c55cbb	Inconsistency alert: - * The OpenSSL names of ciphers with ephemeral DH here include the string - * "DHE", while elsewhere it has always been "EDH". - * (The alias for the list of all such ciphers also is "EDH".) - * The specifications speak of "EDH"; maybe we should allow both forms - * for everything. */ was removed	?			
	ad6019d6c0d22f384838b2f9ca339bdabed331a5	-# error "Inconsistency between crypto.h and cryptlib.c" +# error "Inconsistency between crypto.h and cryptlib.c"	?			
	07481951f9fa7cd8bdd5ee81c7bb1f6bca73d0d1	Correct another inconsistency in my recent commits. was removed from Changelog	N			
	2757c67da2c68d8757cf4314993f7b46f5a351f5	Correct another inconsistency in my recent commits. was added to Changelog	N			
	75871dda4bfb50dd6dd19471114379959a4ea41a	Pointers to them must still be - * ordinary pointers to structs or unions, or the resulting combined - * program will have a type inconsistency. was removed	N			
	2eaabb718b992b8e60979dd044cae78f23767195	Pointers to them must still be + * ordinary pointers to structs or unions, or the resulting combined + * program will have a type inconsistency. was added	N			
	5270e7025e11b2fd1a5bdf8d81feded1167b1c87	Pointers to them must still be + * ordinary pointers to structs or unions, or the resulting combined + * program will have a type inconsistency. was added and	N			
	1d90f280297195f4f1fb42fdeecd0e6f5ee98366	Inconsistency alert: + * The OpenSSL names of ciphers with ephemeral DH here include the string + * "DHE", while elsewhere it has always been "EDH". + * (The alias for the list of all such ciphers also is "EDH".) + * The specifications speak of "EDH"; maybe we should allow both forms + * for everything. */ was added	?			
	3bc90f23737dcf0346b9925a59bcaba60f2bb32f	Rename openssl x509 option '-crlext', which was added in 0.9.5, + to '-clrext' (= clear extensions), as intended and documented. + [Bodo Moeller; inconsistency pointed out by Michael Attili + <attili@amaxo.com>] was added to the CHANGES file	N			
	98e04f9eeb6fcd673a9952fcfab90f38fdf8e7d6	/* Inconsistency alert: cert_chain does include the peer's + * certificate, which we don't include in s3_srvr.c */ was added 2) /* Inconsistency alert: cert_chain does *not* include the + * peer's own certificate, while we do include it in s3_clnt.c */	?			
	62aa714f00c72f20b5c731a7f0a0622ac339c0cc	I'm - making COM-wrappers for selected parts of SSLeay for a project of ours, - and has found this inconsistency in copy semantics annoying." was removed from STATUS file	N			
	2a82c7cf252387b67d79383d518fad4a10bb253e	-# error "Inconsistency between crypto.h and cryptlic.c" +# error "Inconsistency between crypto.h and cryptlib.c"	?			
	d36bcdf5ca819f1f8efb5eb0897f80864e110ad7	# error "Inconsistency between crypto.h and cryptlic.c" was added	?			
	090db4f4750157195c4afb5a9fcb70a4d4eb277e	I'm + making COM-wrappers for selected parts of SSLeay for a project of ours, + and has found this inconsistency in copy semantics annoying." was added in STATUS file	N			
take care	9ddf67f34dd13427d7df5f5169f3c26e6ac06caa	Take care so that none of them can be seen as a script! Flags and their -eventual arguments only! was removed and added	N			
	45c6e23c978da0b23df5e5a9a3c2e631b79ba497	We let the C compiler driver to take care of .s files.was removed	N			
	6d4fb1d59e61aacefa25edc4fe5acfe1ac93f743	Auto-deinit will + * now take care of it so it is no longer required to call this function.	N			
	b8fcd4f079121179f1511fbed5150209c798ce4d	The array reference is a set of arguments for perl rather than the script. +Take care so that none of them can be seen as a script! Flags and their +eventual arguments only! was added	N			
	e84193e43dbd3da23845ef9fcfcb5e364049a396	We let the C compiler driver to take care of .s files.was added	N			

	567a9e6fe0ff3badfa22cf018d87c94ed5a8aeb3	We let the C compiler driver to take care of .s files. was added	N				
	d10dac1187fbb12fdb44a0386f1619b79b40d264	We let the C compiler driver to take care of .s files. was added and removed	N				
	aec27d4d5210234560deab85c97bd453535f66ae	It seems that $switches is getting interpretted with 'eval' or something +# like that, and that we need to take care of backslashes or they will +# disappear along the way. was added	N				
	0f113f3ee4d629ef9a4a30911b22b224772085e5	/* Take care of ODS-5 escapes */ was removed and added 2) /* Take care of the easy one first (eg. it requires no searches) */ was removed and added 3) take care of the rest was removed	N				
	78c990c156ba79521e98728e9a604b4c5cc8adec	# We let the C compiler driver to take care of .s files. was removed	N				
	46a2b3387a3feb044527a58a89555029c809190d	in 64-bit mode I load whole X[16] at once and take care of alignment... was removed and // in sha512 case I load whole X[16] at once and take care of alignment... was added	N				
	975138edaa7f585408db3077db45584a2ba55cd9	We let the C compiler driver to take care of .s files was added	N				
	d64a7232d4c5def7ba9d0b089df71962538d558f	Why folded loop? Because aes[enc|dec] is slow enough to accommodate +# cycles which take care of loop variables... was added	N				
	232a938c75793091285e38efdb941de37eef2725	in 64-bit mode I load whole X[16] at once and take care of alignment... was added	N				
	a2c32e2d7fbd275d22b42532139ef237bc83aa06	Since that's opaque data + all we do is provide a handle to the proper key and let HWCryptoHook + take care of the rest. was added	N				
	1cfd258ed61721ef667ea8a6ca46b57f3765007e	If you want +# to take care of ABI differences yourself, tag functions as +# ".type name,@abi-omnipotent." was added	N				
	a2400fcab884f2851e3e7845c6955a3ddb8bcad4	Take care of ODS-5 escapes */ was added	N				
	1809e858bbc1c3e24ffebdef173871161a036fa6	x86_64 features own ABI I'm not familiar with. Which is why - * I decided to let the compiler take care of subroutine - * prologue/epilogue as well as register allocation. was removed and x86_64 features own ABI which I'm not familiar with. This is + * why I decided to let the compiler take care of subroutine + * prologue/epilogue as well as register allocation. was added	N				
	55b1516770ddd2321f3dda3b81f1ddb671233d3e	We let the C compiler driver to take care of .s files. was removed	N				
	3cc9a89dda7165f9363f06db3559c5dea043bb73	We let the C compiler driver to take care of .s files. was removed and added	N				
	28e276f13928d1db9960acf8449a60b9bf6549c6	We let the C compiler driver to take care of .s files. was added	N				
	2f98abbcb6cfd6ffcf45d5587286f1f849184594	x86_64 features own ABI I'm not familiar with. Which is why + * I decided to let the compiler take care of subroutine + * prologue/epilogue as well as register allocation. was added	N				
	75871dda4bfb50dd6dd19471114379959a4ea41a	Since that's opaque data - all we do is provide a handle to the proper key and let HWCryptoHook - take care of the rest. */ was removed	N				
	5572f482e797a5f6eee34ef7f04a8defde7bdecf	Since that's opaque data + all we do is provide a handle to the proper key and let HWCryptoHook + take care of the rest. was added	N				
	b6d1e52d454bb321153c70cf763945d4b0d4f78e	1) ENGINE in question has asked us to take care of it (ie. the ENGINE did not 2)/* Take care of the easy one first (eg. it requires no searches) */ were added and removed	N				
	8e0a2d846177a7f2dcbec7bf0eb34d76bcd56377	1) ENGINE in question has asked us to take care of it (ie. the ENGINE did not 2) /* Take care of the easy one first (eg. it requires no searches) */ were removed	N				
	14cfde9c83ecfb36711930171ce129293463a83f	1) ENGINE in question has asked us to take care of it (ie. the ENGINE did not 2) /* Take care of the easy one first (eg. it requires no searches) */ were added	N				
	40fcda292f990a25d0ef52d2761be0f20d653e93	1) ENGINE in question has asked us to take care of it (ie. the ENGINE did not 2) /* Take care of the easy one first (eg. it requires no searches) */ were added	N				
	5270e7025e11b2fd1a5bdf8d81feded1167b1c87	Since that's opaque data + all we do is provide a handle to the proper key and let HWCryptoHook + take care of the rest. was added	N				
	b96eb06f7907da2fef89c0c7b89ce4dedc593ecc	We let the C compiler driver to take care of .s files was added	N				
	62ac2938015939e2ef30f12295f0ee59ff79c11b	make sure we have unique states when a program forks - * (new with OpenSSL 0.9.5; for earlier versions, applications - * must take care of this) was removed	N				
	c1e744b9125a883450c2239ec55ea606c618a5c0	/* make sure we have unique states when a program forks + * (new with OpenSSL 0.9.5; for earlier versions, applications + * must take care of this) */ was added	N				
something's gone wrong							
unknown why we ever experience this							
treat this as a soft error							
this isn't quite right							
trial and error							
this doesn't look right							

is this line really safe						
impact of the past design						
impact of the past decision						
quick fix						
better scheme needed	92c78463720f71e47c251ffa58493e32cd793e13	-#ifndef OPENSSL_SYS_MACINTOSH_CLASSIC /* XXXXX: Better scheme needed! [was: #ifndef MAC_OS_pre_X] */ was removed from ssl/ssl.h	**Y**	ssl/ssl.h		2
	4083a229b45df718b7b52994962c5d1ac62b2c8b	-#ifndef OPENSSL_SYS_MACINTOSH_CLASSIC /* XXXXX: Better scheme needed! */ was removed from ssl/ssl_cert.c	**Y**	ssl/ssl_cert.c		109
	a3faebd1041576a59bffe01bbd2c68495870ec5e	1) +#ifndef OPENSSL_SYS_MACINTOSH_CLASSIC /* XXXXX: Better scheme needed! [was: #ifndef MAC_OS_pre_X] */ was added to ssl/ssl.h 2) +#ifndef OPENSSL_SYS_MACINTOSH_CLASSIC /* XXXXX: Better scheme needed! */ was added to ssl/ssl_cert.c	Y	ssl/ssl.h ssl/ssl_cert.c		
You have been warned	7984f082d5045b3a44839b74e4c72877b71ca48f	BIG FSCKING WARNING!!!! If you use this on a statically allocated method - * (that is, it hasn't been allocated using STORE_create_method(), you - * deserve anything Murphy can throw at you and more! You have been warned. was removed	N			
	0f113f3ee4d629ef9a4a30911b22b224772085e5	BIG FSCKING WARNING!!!! If you use this on a statically allocated method - * (that is, it hasn't been allocated using STORE_create_method(), you - * deserve anything Murphy can throw at you and more! You have been warned. was removed and added at multiple places	N			
	ceea4bf047abf369debf5c312928331f107400c6	Let's just say, *I* - * don't use this in a mission-critical environment, so it would be stupid for - * anyone to assume that it is solid and/or tested enough when even its author - * doesn't place that much trust in it. You have been warned. was removed	N			
	ee7ca0941aa245f1f6b01fca03228aabb72c51cb	This stuff is experimental, may change radically or be deleted altogether -before OpenSSL 0.9.7 release. You have been warned! was removed from a README file.	N			
	a5db6fa5760f21d16d59e025e930c02456e00fef	/* BIG FSCKING WARNING!!!! If you use this on a statically allocated method + (that is, it hasn't been allocated using STORE_create_method(), you deserve + anything Murphy can throw at you and more! You have been warned. */ was added	N			
	bc37d996fcfd7f1c7c97728a563a40c0a251d908	This stuff is experimental, may change radically or be deleted altogether +before OpenSSL 0.9.7 release. You have been warned! was added to a README file	N			
	eb929eef147874fc0ca1f172bbd12c6b254fdaec	/* BIG FSCKING WARNING!!!! If you use this on a statically allocated method + (that is, it hasn't been allocated using UI_create_method(), you deserve + anything Murphy can throw at you and more! You have been warned. */ was added	N			
	d1855cc7af56acb62407618711ee5e90a805e231	Let's just say, *I* + * don't use this in a mission-critical environment, so it would be stupid for + * anyone to assume that it is solid and/or tested enough when even its author + * doesn't place that much trust in it. You have been warned. was added	N			
a really bad idea	5998e2903589e7b19e102ebff06521f2dcb60409	/* - * This function seems like a really bad idea. Should we remove it - * completely? - */ was removed from ssl/statem/statem.c	**Y**	ssl/statem/statem.c		10
	8ba708e5166b02ab61f2762d36b3e7b7455e9c06	/* - * This function seems like a really bad idea. Should we remove it - * completely? - */ was removed from ssl/statem.c [DF] and added to ssl/statem/statem.c[NF]	Y	ssl/statem.c ssl/statem/statem.c	1aeaa7ec06ccd4c819a3ca94139c3ab79463fada	2251
	49ae742398aecd81551d59f421e4116a5b8a4ea9	/* + * This function seems like a really bad idea. Should we remove it + * completely? + */ was added to ssl/statem.c	Y	ssl/statem.c		
						Total : 29