1. CODE REVIEW: BeeCrypt

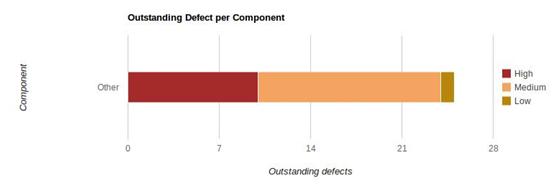
Method of analysis

BeeCrypt is a library to provide strong and fast cryptographic functions. It is a big project developed over a long period of time since year 2000, with more than 67K lines. We used CppCheck and Coverity scan to perform the analysis of this project.

Results:

Cppcheck: CppCheck test result shows many style warnings in the code. All of these warnings are about the functions not being used. Because BeeCrypt is a library, existence of such functions is expected. Even then a thorough analysis of these functions can be done to ensure any possible misuse from these functions. Details of this analysis are appended in Appendix.

Coverity scan: Coverity scan reported 25 defects. It includes uninitialized variables, memory corruptions, memory-illegal access, API usage errors, control flow issues, integer handling issues and some other low impact defects.



# Conclusion:

BeeCrypt is a library under development and it has matured over time. This is clearly visible in the test results as obtained by CppCheck and Coverity scan. Coverity scan could find only 25 possible problems in complete code.

Appendix

**CppCheck report:**

[beecrypt.c:943]: (style) The function 'DllMain' is never used.

[base64.c:326]: (style) The function 'b64crc' is never used.

[base64.c:355]: (style) The function 'b64decode' is never used.

[base64.c:48]: (style) The function 'b64enc' is never used.

[beecrypt.c:906]: (style) The function 'blockCipherContextCBC' is never used.

[beecrypt.c:925]: (style) The function 'blockCipherContextCTR' is never used.

[beecrypt.c:887]: (style) The function 'blockCipherContextECB' is never used.

[beecrypt.c:844]: (style) The function 'blockCipherContextSetCTR' is never used.

[beecrypt.c:828]: (style) The function 'blockCipherContextSetIV' is never used.

[beecrypt.c:873]: (style) The function 'blockCipherContextValidKeylen' is never used.

[beecrypt.c:755]: (style) The function 'blockCipherCount' is never used.

[dhies.c:294]: (style) The function 'dhies\_pContextDecrypt' is never used.

[dhies.c:244]: (style) The function 'dhies\_pContextEncrypt' is never used.

[dhies.c:159]: (style) The function 'dhies\_pContextFree' is never used.

[dhies.c:139]: (style) The function 'dhies\_pContextInitDecrypt' is never used.

[dhies.c:149]: (style) The function 'dhies\_pContextInitEncrypt' is never used.

[dldp.c:91]: (style) The function 'dldp\_pPair\_s' is never used.

[dldp.c:42]: (style) The function 'dldp\_pPrivate' is never used.

[dldp.c:55]: (style) The function 'dldp\_pPrivate\_s' is never used.

[dldp.c:68]: (style) The function 'dldp\_pPublic' is never used.

[dldp.c:446]: (style) The function 'dldp\_pgonGenerator' is never used.

[dldp.c:317]: (style) The function 'dldp\_pgonMake' is never used.

[dldp.c:347]: (style) The function 'dldp\_pgonMakeSafe' is never used.

[dldp.c:285]: (style) The function 'dldp\_pgoqGenerator' is never used.

[dldp.c:223]: (style) The function 'dldp\_pgoqMakeSafe' is never used.

[dlkp.c:70]: (style) The function 'dlkp\_pCopy' is never used.

[dlkp.c:57]: (style) The function 'dlkp\_pFree' is never used.

[dlkp.c:46]: (style) The function 'dlkp\_pInit' is never used.

[dlkp.c:34]: (style) The function 'dlkp\_pPair' is never used.

[dlpk.c:58]: (style) The function 'dlpk\_pCopy' is never used.

[dlpk.c:68]: (style) The function 'dlpk\_pEqual' is never used.

[dlpk.c:48]: (style) The function 'dlpk\_pFree' is never used.

[dlpk.c:38]: (style) The function 'dlpk\_pInit' is never used.

[dlpk.c:90]: (style) The function 'dlpk\_pgonValidate' is never used.

[dlpk.c:74]: (style) The function 'dlpk\_pgoqValidate' is never used.

[dsa.c:173]: (style) The function 'dsaparamMake' is never used.

[dsa.c:34]: (style) The function 'dsasign' is never used.

[dsa.c:96]: (style) The function 'dsavrfy' is never used.

[elgamal.c:34]: (style) The function 'elgv1sign' is never used.

[elgamal.c:71]: (style) The function 'elgv1vrfy' is never used.

[elgamal.c:115]: (style) The function 'elgv3sign' is never used.

[elgamal.c:148]: (style) The function 'elgv3vrfy' is never used.

[beecrypt.c:88]: (style) The function 'entropySourceCount' is never used.

[beecrypt.c:476]: (style) The function 'hashFunctionContextDigestMatch' is never used.

[beecrypt.c:367]: (style) The function 'hashFunctionContextUpdateMC' is never used.

[beecrypt.c:269]: (style) The function 'hashFunctionCount' is never used.

[beecrypt.c:679]: (style) The function 'keyedHashFunctionContextDigest' is never used.

[beecrypt.c:591]: (style) The function 'keyedHashFunctionContextReset' is never used.

[beecrypt.c:605]: (style) The function 'keyedHashFunctionContextUpdate' is never used.

[beecrypt.c:639]: (style) The function 'keyedHashFunctionContextUpdateMP' is never used.

[beecrypt.c:504]: (style) The function 'keyedHashFunctionCount' is never used.

[memchunk.c:104]: (style) The function 'memchunkClone' is never used.

[memchunk.c:68]: (style) The function 'memchunkFree' is never used.

[memchunk.c:51]: (style) The function 'memchunkInit' is never used.

[memchunk.c:57]: (style) The function 'memchunkWipe' is never used.

[mpbarrett.c:858]: (style) The function 'mpbbits' is never used.

[mpbarrett.c:391]: (style) The function 'mpbneg' is never used.

[mpbarrett.c:792]: (style) The function 'mpbnmulmod' is never used.

[mpbarrett.c:845]: (style) The function 'mpbnpowmodsld' is never used.

[mpbarrett.c:813]: (style) The function 'mpbnsqrmod' is never used.

[mpbarrett.c:736]: (style) The function 'mpbpprime\_w' is never used.

[mpbarrett.c:153]: (style) The function 'mpbsetbin' is never used.

[mpbarrett.c:192]: (style) The function 'mpbsethex' is never used.

[mpnumber.c:266]: (style) The function 'mpnbits' is never used.

[mpnumber.c:74]: (style) The function 'mpninit' is never used.

[mpnumber.c:182]: (style) The function 'mpnsethex' is never used.

[pkcs12.c:5]: (style) The function 'pkcs12\_derive\_key' is never used.

[pkcs1.c:34]: (style) The function 'pkcs1\_emsa\_encode\_digest' is never used.

[blockpad.c:34]: (style) The function 'pkcs5Pad' is never used.

[blockpad.c:92]: (style) The function 'pkcs5UnpadCopy' is never used.

[beecrypt.c:217]: (style) The function 'randomGeneratorContextFree' is never used.

[beecrypt.c:195]: (style) The function 'randomGeneratorContextInit' is never used.

[beecrypt.c:242]: (style) The function 'randomGeneratorContextNext' is never used.

[beecrypt.c:247]: (style) The function 'randomGeneratorContextSeed' is never used.

[beecrypt.c:160]: (style) The function 'randomGeneratorCount' is never used.

[rsakp.c:178]: (style) The function 'rsakpCopy' is never used.

[rsakp.c:157]: (style) The function 'rsakpFree' is never used.

[rsakp.c:140]: (style) The function 'rsakpInit' is never used.

[rsakp.c:39]: (style) The function 'rsakpMake' is never used.

[rsapk.c:57]: (style) The function 'rsapkCopy' is never used.

[rsapk.c:49]: (style) The function 'rsapkFree' is never used.

[rsapk.c:38]: (style) The function 'rsapkInit' is never used.

[rsa.c:58]: (style) The function 'rsapri' is never used.

[rsa.c:81]: (style) The function 'rsapricrt' is never used.

[rsa.c:35]: (style) The function 'rsapub' is never used.

[rsa.c:152]: (style) The function 'rsavrfy' is never used.

[endianness.c:44]: (style) The function 'swap16' is never used.

[endianness.c:56]: (style) The function 'swap32' is never used.

[endianness.c:72]: (style) The function 'swap64' is never used.

[timestamp.c:44]: (style) The function 'timestamp' is never used.