Issues for QAT20_WIN_MAIN

Search query: severity:1,2,3,4

View: *default*

#192: Risky cryptographic algorithm MD2 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:193 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#193: Array 'L"ECDSA_P521"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdsaprov\ecdsaprov.c:1361 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#194: Resource acquired to 'hdlllockey' at line 625 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_igzip.c:652 | GetISALDllLocation()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#195: function 'wprintf' possibly accepts format string that may be influenced by user, causing format string vulnerability. Undefined string lengths can lead to buffer overflows and potential exploitation by attackers. Use a defined value for string lengths.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:289 | SetupDriverName()
Code: SV.FMTSTR.GENERIC | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#196: wprintf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:289 | SetupDriverName()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#198: Array 'pBuf' of size '(SizeOfAlgId+20)-400' may use index value(s) 0..SizeOfAlgId-1
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:173 | FillInPaddingInfo()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#199: Array 'L"DSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\dsa\dsaprov.c:1889 | CpmAddDsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#201: Address of a local variable is returned through formal argument 'pDst->lastEncRoundKey'.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalAESKey.c:308 | SymCryptAesKeyCopy()
Code: LOCRET.ARG | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#202: Array 'pKey->cpmCommon.szAlgName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:467 | CpmCommonImportKeyPair()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#205: Array 'L"RSA_SIGN"' of size 9 may use index value(s) 9..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:3126 | CpmAddRsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#206: Array 'L"ECDSA_P384"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdsaprov\ecdsaprov.c:1359 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#208: 'inputParams.processingSize' might be used in a division by zero
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3206 | main()
Code: DBZ.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#209: Array 'L"SHA512"' of size 7 may use index value(s) 7..16. Also there are 2 similar errors on lines 663, 680.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonKdf.c:647 | KdfSP800Impl()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#210: Array 'pAlgorithm->szAlgName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonProvider.c:536 | CpmCommonOpenProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#211: Array 'key' of size 128 may use index value(s) -1
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_c3xxx\adf_c3xxx_hw_data.c:427 | get_storage_enabled()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#212: Resource acquired to 'overlapped.hEvent' at line 425 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:484 | compressBufferQatCrc64()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#213: Array 'HashAlgName' of size 16 may use index value(s) -1..0. Also there are 7 similar errors on lines 647, 653, 658, 663, 670, 675, 680.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonKdf.c:640 | KdfSP800Impl()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#214: Array 'L"SHA384"' of size 7 may use index value(s) 7..16. Also there is one similar error on line 675.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonKdf.c:658 | KdfSP800Impl()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#216: Risky cryptographic algorithm MD4 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:200 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#217: Null pointer 'pResponse' that comes from line 443 may be dereferenced at line 548. Also there are 2 similar errors on lines 783, 862.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\compression\dc_datapath.c:548 | dcCompression_ProcessCallback()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#218: wprintf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:415 | InstallDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#220: Array 'L"ECDH_P384"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdh\ecdhprov.c:1171 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#221: Array 'pKey->cpmCommon.szAlgName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:244 | CpmCommonGenerateKeyPair()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#222: Array 'L"ECDSA_P521"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:1780 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#224: Array 'L"ECDSA_P256"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:1776 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#225: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\AesTest.c:863 | RSAKeyGenTest()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#227: 'aes' is used uninitialized in this function.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_c62x\adf_c62x_hw_data.c:127 | get_sku()
Code: UNINIT.STACK.MUST | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#228: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:3125 | CpmAddRsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#229: Array 'pAlg->szAlgName' of size 64 may use index value(s) 64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:244 | CpmCommonGenerateKeyPair()
Code: ABV.MEMBER | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#230: printf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'. Also there is one similar error on line 485.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:462 | RemoveDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#231: Risky cryptographic algorithm MD4 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:248 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#232: Resource acquired to 'key' at line 87 may be lost here.

C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\asymmprov.c:147 | LoadConfig()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#233: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\AesTest.c:1063 | SignTest()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#234: Array 'L"ECDH_P521"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdh\ecdhprov.c:1173 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#235: Risky cryptographic algorithm MD5 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalCryptoInterface.c:113 | OsalServicesInit()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#236: Array 'L"RSA_SIGN"' of size 9 may use index value(s) 9..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\rsaprov\rsaprov.c:2321 | CpmAddRsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#239: Null pointer 'pAlgName' that comes from line 873 may be passed to function and can be dereferenced there by passing argument 1 to function '_memcpy_s' at line 969.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\kdf\kdf_tls.c:969 | KdfTLSImpl()
Code: NPD.GEN.CALL.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#240: printf format specification '%S' expects type 'wchar_t*' for 'S', but parameter 2 has incompatible type 'WCHAR*'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:313 | SetupDriverName()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#241: Resource acquired to 'fileHandle' at line 236 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:251 | SetupUModeFileName()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#242: Array 'L"ECDH_P521"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh\ecdhprov.c:1619 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#243: Null pointer 'hashAlgName' that comes from line 873 may be dereferenced at line 1108. Also there are 3 similar errors on lines 1108, 1120.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\kdf\kdf_tls.c:1108 | KdfTLSImpl()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#246: Resource acquired to 'Overlap.hEvent' at line 1305 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\CommonIoctl.c:1337 | CpmOverlappedDeviceIoControl()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#247: Possible memory leak. Dynamic memory stored in 'pQzPrivateCtx' allocated through function 'calloc' at line 283 can be lost at line 392
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\xpress.c:392 | xpressSetupSession()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#248: Array 'L"ECDSA_P384"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:1778 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#249: Array 'L"ECDH_P256"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh\ecdhprov.c:1615 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#251: Non-void function does not return value
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\adf_dev_mgr.c:465 | adf_dev_in_use()
Code: FUNCRET.GEN | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#252: Array 'adfInsts' of size 1024 may use index value(s) 1024..2046
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\ctrl\sal_compression.c:2456 | dcGetFirstHandle()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#253: Null pointer 'pCdInfoOptimised' that comes from line 1615 may be dereferenced at line 2248.

C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\crypto\sym\lac_sym_alg_chain.c:2248 | LacAlgChain_SessionInit()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#255: Array 'pExpandedKey->RoundKey[0]' of size 16 may use index value(s) 16..23. Also there is one similar error on line 208.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalAESKey.c:177 | SymCryptAesExpandKeyInternal()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#256: Array 'revKey.RoundKey[0]' of size 16 may use index value(s) 16..111
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalCryptoInterface.c:665 | osalAESKeyExpansionForward()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#257: Array 'pbBuffer' of size 18 may use index value(s) 0..37
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh2\ecdh2prov.c:1303 | CpmEcdh2GetMetaData()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#259: Array 'key' of size 128 may use index value(s) -1
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\adf_adi.c:149 | adf_init_adis()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#261: 'totalvfs' is used uninitialized in this function.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_4xxx\adf_4xxx_hw_data.c:249 | check_arbitrary_numvfs()
Code: UNINIT.STACK.MUST | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#264: function 'wprintf' possibly accepts format string that may be influenced by user, causing format string vulnerability. Undefined string lengths can lead to buffer overflows and potential exploitation by attackers. Use a defined value for string lengths.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:222 | SetupUModeFileName()
Code: SV.FMTSTR.GENERIC | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#265: Resource acquired to 'fileHandle' at line 303 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:319 | SetupDriverName()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#266: printf format specification '%ls' expects type 'wchar_t*' for 's', but parameter 3 has incompatible type 'LPCTSTR'. Also there is one similar error on line 374.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:374 | InstallDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#267: Array 'pAlg->szAlgName' of size 64 may use index value(s) 64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:467 | CpmCommonImportKeyPair()
Code: ABV.MEMBER | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#268: Array 'node->algName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonProvider.c:242 | AddCommonProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#269: Non-void function does not return value
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\adf_dev_mgr.c:62 | adf_get_vf_num()
Code: FUNCRET.GEN | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#271: Resource acquired to 'overlapped.hEvent' at line 342 may be lost here. Also there is one similar error on line 398.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:398 | compressBufferQat()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#272: function 'stat' operates on file names and is vulnerable to race conditions. Files can be manipulated by attackers between creation and access time.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:2704 | main()
Code: SV.TOCTOU.FILE_ACCESS | Severity: Review (4) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#274: wprintf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:222 | SetupUModeFileName()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#275: Array 'pPrivKey->cpmCommon.szAlgName' of size 64 may use index value(s) 64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:618 | CpmCommonSecretAgreement()

Code: ABV.MEMBER | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#276: printf format specification '%ls' expects type 'wchar_t*' for 's', but parameter 2 has incompatible type 'LPCTSTR'. Also there are 2 similar errors on lines 528, 558.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:519 | StartDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#278: Array '&ctx_mask' of size 1 may use index value(s) 1..7
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\qat_hal.c:1772 | qat_hal_init_wr_xfer()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#279: Array 'buffer' of size 14 may use index value(s) 0..29
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:1754 | CpmEcdsaGetMetaData()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#280: 'sku' is used uninitialized in this function.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_dh895xcc\adf_dh895xcc_hw_data.c:118 | get_sku()
Code: UNINIT.STACK.MUST | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#281: 'aes' is used uninitialized in this function.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_c3xxx\adf_c3xxx_hw_data.c:119 | get_sku()
Code: UNINIT.STACK.MUST | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#282: Null pointer 'pTlsSeed' that comes from line 872 may be passed to function and can be dereferenced there by passing argument 1 to function '_memcpy_s' at line 985.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\kdf\kdf_tls.c:985 | KdfTLSImpl()
Code: NPD.GEN.CALL.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#285: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\rsaprov\rsaprov.c:2319 | CpmAddRsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#286: Array 'pbBuffer' of size 13 may use index value(s) 0..27
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\dh\dhprov.c:359 | CpmDhGetMetaData()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#287: Array 'L"DH"' of size 3 may use index value(s) 3..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\dh\dhprov.c:525 | CpmAddDhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#289: Unvalidated string '*argv' is received from an external function through a call to 'main' at line 2583 and can be used in a potential security decision through call to 'Parse' at line 2638.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:2638 | main()
Code: SV.TAINTED.SECURITY_DECISION | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#291: Array 'L"ECDSA_P256"' of size 11 may use index value(s) 11..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdsaprov\ecdsaprov.c:1357 | CpmAddEcdsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#293: Array 'key' of size 128 may use index value(s) -1
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_dh895xcc\adf_dh895xcc_hw_data.c:519 | get_storage_enabled()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#294: Resource acquired to 'overlapped.hEvent' at line 1305 may be lost here. Also there is one similar error on line 1371.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:1371 | getQatHwAlgorithms()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#295: Array 'CurveName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\eccurves.c:708 | IsCurveNameSupported()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#296: Resource acquired to 'overlapped.hEvent' at line 619 may be lost here. Also there is one similar error on line 671.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:671 | decompressBufferQat()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#299: function 'wprintf' possibly accepts format string that may be influenced by user, causing format string vulnerability. Undefined string lengths can lead to buffer overflows and potential exploitation by attackers. Use a defined value for string lengths.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:120 | ManageDriver()
Code: SV.FMTSTR.GENERIC | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#300: printf format specification '%S' expects type 'wchar_t*' for 'S', but parameter 2 has incompatible type 'WCHAR*'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:245 | SetupUModeFileName()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#301: Null pointer 'pMsBlob' that comes from line 276 may be dereferenced at line 333. Also there is one similar error on line 338.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdsaprov\ecdsa2prov.c:333 | CpmEcdsa2ImportKeyPairImpl()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#303: Risky cryptographic algorithm MD5 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:255 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#305: Risky cryptographic algorithm SHA-1 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:262 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#306: Array 'L"DH"' of size 3 may use index value(s) 3..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\dh\dhprov.c:1573 | CpmAddDhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#307: Array 'L"ECDH_P256"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\ecdh\ecdhprov.c:1169 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#308: function 'fopen' operates on file names and is vulnerable to race conditions. Files can be manipulated by attackers between creation and access time. Also there are 2 similar errors on lines 2942, 2952.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:2735 | main()
Code: SV.TOCTOU.FILE_ACCESS | Severity: Review (4) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#310: Address of a local variable is returned through formal argument 'pDst->lastDecRoundKey'.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalAESKey.c:308 | SymCryptAesKeyCopy()
Code: LOCRET.ARG | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#313: Array 'CurveName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\eccurves.c:736 | FindCurveByName()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#314: Array 'L"DSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\dsa\dsaprov.c:520 | CpmAddDsaProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#315: Array 'L"SHA256"' of size 7 may use index value(s) 7..16. Also there are 2 similar errors on lines 653, 670.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonKdf.c:640 | KdfSP800Impl()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#316: Array 'EccName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\eccurves.c:1102 | InitializeCurveParamTable()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#317: Array 'adfInsts' of size 1024 may use index value(s) 0..2046. Also there are 4 similar errors on lines 3624, 3629, 3633, 3638.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\ctrl\sal_crypto.c:3620 | Lac_GetFirstHandle()
Code: ABV.STACK | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#318: Null pointer 'pCookie' that comes from line 505 may be dereferenced at line 796. Also there are 2 similar errors on lines 894, 897.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\compression\dc_datapath.c:796 | dcCompression_ProcessCallback()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#319: Array '&ctx_mask' of size 1 may use index value(s) 1..7
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\qat_hal.c:1807 | qat_hal_init_rd_xfer()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#321: Unvalidated integer value 'dosHeader->e_lfanew' that is received from 'ReadFile' at line 717 is used as an operand to a binary operator at line 734.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_igzip.c:734 | getIGZipDllVersion()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#322: Array 'jobs' of size 511 may use index value(s) 511..8175. Also there is one similar error on line 675.

C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\cf_qat_back\cf_qat_back.c:674 | cfQatUsePreallocFlatBuffers()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#323: Risky cryptographic algorithm MD5 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:207 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#324: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\AesTest.c:686 | RSATest()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#325: Array 'pbBuffer' of size 18 may use index value(s) 0..37
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsa2prov.c:219 | CpmEcdsa2GetMetaData()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#326: Array 'pbBuffer' of size 14 may use index value(s) 0..29
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh\ecdhprov.c:1168 | CpmEcdhGetMetaData()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#327: Risky cryptographic algorithm MD2 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:241 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#328: Array 'pSecret->cpmCommon.szAlgName' of size 64 may use index value(s) -1..0
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonAsymm.c:618 | CpmCommonSecretAgreement()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#329: Risky cryptographic algorithm SHA-1 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:214 | InitializeCommonUtils()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#331: wprintf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:120 | ManageDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#332: Array 'key' of size 128 may use index value(s) -1
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_c62x\adf_c62x_hw_data.c:472 | get_storage_enabled()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#333: Expression 'IoControlCode' can never reach the value '((((0x9000+0))<<16)|((0)<<14)|((0x901)<<2)|(2))' = -1879038970
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\cf_qat_back\cf_qat_back_ioctl.c:348 | CfQatEvtIoDeviceControl()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#334: printf format specification '%x' expects type 'unsigned int' for 'x', but parameter 2 has incompatible type 'UINT'. Also there is one similar error on line 623.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:602 | StopDriver()
Code: SV.FMT_STR.PRINT_FORMAT_MISMATCH.BAD | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#337: Array '&ctx_mask' of size 1 may use index value(s) 1..7
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\qat_hal.c:1738 | qat_hal_init_gpr()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#339: Array 'L"ECDH_P384"' of size 10 may use index value(s) 10..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh\ecdhprov.c:1617 | CpmAddEcdhProvider()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#340: Risky cryptographic algorithm SHA-1 is used
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\osal\src\windows\kernel_space\OsalCryptoInterface.c:120 | OsalServicesInit()
Code: RCA | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#341: Null pointer 'pTlsLabel' that comes from line 871 may be passed to function and can be dereferenced there by passing argument 1 to function '_memcpy_s' at line 977.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\kdf\kdf_tls.c:977 | KdfTLSImpl()
Code: NPD.GEN.CALL.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#342: Array 'L"RSA"' of size 4 may use index value(s) 4..64
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\cpmprov\AesTest.c:897 | RSAPerfTest()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#344: function 'wprintf' possibly accepts format string that may be influenced by user, causing format string vulnerability. Undefined string lengths can lead to buffer overflows and potential exploitation by attackers. Use a defined value for string lengths.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\CNGInstaller\install.cpp:415 | InstallDriver()
Code: SV.FMTSTR.GENERIC | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#347: Array 'init_status' of size 32 may use index value(s) 32..134217727
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\adf_init.c:821 | adf_dev_shutdown_locked()
Code: ABV.GENERAL | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#349: The result of expression: 'size+0x1000' generates 4-byte type while casting to a bigger size of 8-byte
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\windows_adf\Adf\adf_osa_windows.h:627 | _MY_PAGE_ALIGN()
Code: NUM.OVERFLOW | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#352: Non-void function does not return value
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_4xxx\adf_4xxx_tl.c:21 | get_tl_num_desc()
Code: FUNCRET.GEN | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#353: 'tl_rp_data' is used uninitialized in this function.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_4xxx\adf_4xxx_tl.c:143 | adf_create_tl_desc()
Code: UNINIT.STACK.MUST | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#355: Resource acquired to 'overlapped.hEvent' at line 716 may be lost here. Also there is one similar error on line 772.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:772 | compressBufferMetadata()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#360: Expression 'IoControlCode' can never reach the value '((((0x9000+0))<<16)|((0)<<14)|((0x901)<<2)|(2))' = -1879038970
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\cf_qat_back\cf_qat_back_ioctl.c:525 | CfFastIoDeviceControl()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#361: Expression 'IoControlCode' can never reach the value '((((0x9000+0))<<16)|((0)<<14)|((0x907)<<2)|(2))' = -1879038946
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\cf_qat_back\cf_qat_back_ioctl.c:526 | CfFastIoDeviceControl()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#362: Resource acquired to 'overlapped.hEvent' at line 800 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:859 | decompressBufferQatCrc64()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#363: Non-void function does not return value
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\adf\drivers\crypto\qat\qat_common\adf_dev_mgr.c:56 | adf_get_vf_id()
Code: FUNCRET.GEN | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#365: Expression '_exception_code()' can never reach the value '((NTSTATUS)0xC0000005L)' = -1073741819
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\qz_metadata.c:213 | qzCompressWithMetadataExt()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#367: Suspicious dereference of pointer 'pCookie' before NULL check at line 2753
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\sal\me_acceleration_layer\access_layer\look_aside_acceleration\src\common\crypto\sym\lac_sym_alg_chain.c:2630 | LacAlgChain_Perform()
Code: RNPD.DEREF | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#375: The result of expression: 'bank_nr*0x2000' generates 4-byte type while casting to a bigger size of 8-byte
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\windows_adf\Adf\lac_adf_interface_stub.c:190 | icp_adf_transCreateHandle()
Code: NUM.OVERFLOW | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#377: The result of expression: 'bank_nr*0x2000' generates 4-byte type while casting to a bigger size of 8-byte
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\windows_adf\Adf\lac_adf_interface_stub.c:278 | icp_adf_transCreateHandle()
Code: NUM.OVERFLOW | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#379: The result of expression: 'bank_nr*0x2000' generates 4-byte type while casting to a bigger size of 8-byte

C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\windows_adf\Adf\Iac_adf_interface_stub.c:234 | icp_adf_transCreateHandle()
Code: NUM.OVERFLOW | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#385: Unvalidated integer value 'cur_unc_err_time.QuadPart' that is received from '0x18446734727860715540' at line 365 is used as an operand to a binary operator at line 368.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\windows_adf\Adf\adf_isr_windows.c:368 | CountUncorrectableErrorAndQueueDpc()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#502: Possible memory leak. Dynamic memory stored in 'RSSignParam.m.pData' allocated through function 'HeapAlloc' at line 598 can be lost at line 709
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:709 | CpmEcdsaSignHash_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#503: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep1.modulusN.pData' allocated through function 'HeapAlloc' at line 766 can be lost at line 938
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:938 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#504: Possible memory leak. Dynamic memory stored in 'Y.pData' allocated through function 'HeapAlloc' at line 1112 can be lost at line 1177
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprime.c:1177 | RsaGenerateLargePrime()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#507: Expression 'status' can never reach the value '((DWORD)0xC000000DL)' = 3221225485
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\common\CommonUtils.c:895 | CpmAddFlatBuffer()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#516: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.coefficientQInv.pData' allocated through function 'HeapAlloc' at line 1164 can be lost at line 1227. Also there is one similar error on line 1227.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1227 | CpmRsaSaveKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#518: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.exponent1Dp.pData' allocated through function 'HeapAlloc' at line 1141 can be lost at line 1225. Also there is one similar error on line 1225.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1225 | CpmRsaSaveKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#519: Possible memory leak. Dynamic memory stored in 'RSSignParam.m.pData' allocated through function 'HeapAlloc' at line 950 can be lost at line 1054
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsa2prov.c:1054 | CpmEcdsa2SignHash_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#525: Null pointer 'pMsBlob' that comes from line 299 may be dereferenced at line 356. Also there is one similar error on line 361.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsa2prov.c:356 | CpmEcdsa2SaveKeyPair_UQ()
Code: NPD.GEN.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#526: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.coefficientQInv.pData' allocated through function 'HeapAlloc' at line 754 can be lost at line 934
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:934 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#527: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.exponent2Dq.pData' allocated through function 'HeapAlloc' at line 760 can be lost at line 936
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:936 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#531: Expression 'ntStatus' can never reach the value '((DWORD)0xC0000017L)' = 3221225495
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprime.c:477 | CheckCoprime()
Code: CWARN.NOEFFECT.OUTOFRANGE | Severity: Warning (3) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#535: Possible memory leak. Dynamic memory stored in 'xp1.pData' allocated through function 'HeapAlloc' at line 781 can be lost at line 921
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:921 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#539: Possible memory leak. Dynamic memory stored in 'R2.pData' allocated through function 'HeapAlloc' at line 580 can be lost at line 636
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprime.c:636 | RsaGenerateRValue()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#540: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.exponent2Dq.pData' allocated through function 'HeapAlloc' at line 1152 can be lost at line 1226. Also there is one similar error on line 1226.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1226 | CpmRsaSaveKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#543: Possible memory leak. Dynamic memory stored in 'xp2.pData' allocated through function 'HeapAlloc' at line 782 can be lost at line 922
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:922 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#547: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep1.privateExponentD.pData' allocated through function 'HeapAlloc' at line 763 can be lost at line 937
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:937 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#551: Possible memory leak. Dynamic memory stored in 'k_data.pData' allocated through function 'HeapAlloc' at line 1436 can be lost at line 1437
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdh2\ecdh2prov.c:1437 | Ecdh2CalcSecret()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#557: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.prime2Q.pData' allocated through function 'HeapAlloc' at line 751 can be lost at line 933
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:933 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#561: Possible memory leak. Dynamic memory stored in 'mult2P1P2.pData' allocated through function 'HeapAlloc' at line 701 can be lost at line 912
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprime.c:912 | RsaGeneratePValue()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#562: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.exponent1Dp.pData' allocated through function 'HeapAlloc' at line 757 can be lost at line 935
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:935 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#586: Resource acquired to 'overlapped.hEvent' at line 514 may be lost here.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\qatzip\cf_qat.c:576 | compressBufferQatCrc64SW()
Code: RH.LEAK | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#590: Object 'CoprimeVals.pData' was used at line 481 after being freed by calling 'HeapFree' at line 451
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprime.c:481 | CheckCoprime()
Code: UFM.USE.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#601: Unvalidated integer value '(double)uncompressedBufferSize*8.000000* (double)numIterations' that is received from 'Parse' at line 2638 is used as an operand to a binary operator at line 3235.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3235 | main()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#602: Unvalidated integer value 'numIterations' that is received from 'Parse' at line 2638 is used as an operand to a binary operator at line 3235. Also there is one similar error on line 3239.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3235 | main()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#603: Unvalidated integer value 'inputParams.numIterations' that is received from 'Parse' at line 2638 is used as an operand to a binary operator at line 3089. Also there is one similar error on line 3358.

C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3089 | main()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#604: Unvalidated integer value '(double)uncompressedBufferSize*8.000000* (double)numIterations* (double)threadThroughputMultiplier' that is received from 'Parse' at line 2638 is used as an operand to a binary operator at line 3234.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3234 | main()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#605: Unvalidated integer value 'inputParams.numIterations' is received from 'Parse' at line 2638 and can be used in a loop condition through a call to 'printThreadedStats' at line 3407.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3407 | main()
Code: SV.TAINTED.CALL.LOOP_BOUND | Severity: Error (2) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#607: Unvalidated integer value 'inputParams.numIterations' that is received from 'Parse' at line 2638 is used as an operand to a binary operator via a call to 'printThreadedStats' at line 3407.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3407 | main()
Code: SV.TAINTED.CALL.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#621: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep1.privateExponentD.pData' allocated through function 'HeapAlloc' at line 1132 can be lost at line 1224. Also there is one similar error on line 1224.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1224 | CpmRsaSaveKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#622: Pointer 'pKey->privKey.privateKeyRep1.privateExponentD.pData' returned from call to function 'HeapAlloc' at line 763 may be NULL and may be dereferenced at line 764.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:764 | CpmRsaFinalizeKeyPair_UQ()
Code: NPD.FUNC.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#623: Pointer 'pKey->privKey.privateKeyRep1.modulusN.pData' returned from call to function 'HeapAlloc' at line 766 may be NULL and may be dereferenced at line 767.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:767 | CpmRsaFinalizeKeyPair_UQ()
Code: NPD.FUNC.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#624: Pointer 'pKey->privKey.privateKeyRep2.exponent1Dp.pData' returned from call to function 'HeapAlloc' at line 1141 may be NULL and may be dereferenced at line 1142.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1142 | CpmRsaSaveKeyPair_UQ()
Code: NPD.FUNC.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#625: Pointer 'pKey->privKey.privateKeyRep2.coefficientQInv.pData' returned from call to function 'HeapAlloc' at line 1164 may be NULL and may be dereferenced at line 1165.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1165 | CpmRsaSaveKeyPair_UQ()
Code: NPD.FUNC.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#626: Possible memory leak. Dynamic memory stored in 'VerifyParam.m.pData' allocated through function 'HeapAlloc' at line 877 can be lost at line 973
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsaprov.c:973 | CpmEcdsaVerifySignature_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#627: Possible memory leak. Dynamic memory stored in 'pKey->privKey.privateKeyRep2.prime1P.pData' allocated through function 'HeapAlloc' at line 748 can be lost at line 932
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:932 | CpmRsaFinalizeKeyPair_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#628: Possible memory leak. Dynamic memory stored in 'VerifyParam.m.pData' allocated through function 'HeapAlloc' at line 1213 can be lost at line 1309
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\ecdsaprov\ecdsa2prov.c:1309 | CpmEcdsa2VerifySignature_UQ()
Code: MLK.MIGHT | Severity: Error (2) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#630: Pointer 'pKey->privKey.privateKeyRep2.exponent2Dq.pData' returned from call to function 'HeapAlloc' at line 1152 may be NULL and may be dereferenced at line 1153.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\crypto\BCrypt\UCpmProvider\rsaprov\rsaprov.c:1153 | CpmRsaSaveKeyPair_UQ()
Code: NPD.FUNC.MIGHT | Severity: Critical (1) | State: Existing | Status: Not a Problem | Taxonomy: C and C++ | Owner: unowned

#641: Unvalidated integer value 'crcNumIterations' is received from 'Parse' at line 2638 and can be used in a loop condition at line 3432.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3432 | main()
Code: SV.TAINTED.LOOP_BOUND | Severity: Error (2) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#642: Unvalidated integer value 'crcNumIterations' is received from 'Parse' at line 2638 and can be used to alter memory allocation size through call to 'calloc' at line 2865.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:2865 | main()
Code: SV.TAINTED.ALLOC_SIZE | Severity: Error (2) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned

#643: Unvalidated integer value '(double)blockCount* (double)numIterations' that is received from 'Parse' at line 2638 is used as an operand to a binary operator at line 3238.
C:\jenkins_root\workspace\QAT\WIN\QAT20\QAT20-MAIN_KW\compression\parcomp\main.c:3238 | main()
Code: SV.TAINTED.BINOP | Severity: Warning (3) | State: Existing | Status: Analyze | Taxonomy: C and C++ | Owner: unowned