Additional fixes #10116

Merged douzzer merged 5 commits into `wolfSSL:master` from `Frauschi:zd21457` 3 days ago

Conversation Commits 5 Checks Files changed

Frauschi commented last week — Contributor

zd21457

Frauschi added the For This Release label last week

Frauschi requested a review from **wolfSSL-Fenrir-bot** last week

wolfSSL-Fenrir-bot reviewed last week

View reviewed changes

wolfSSL-Fenrir-bot left a comment

Fenrir Automated Review — PR #10116

Scan targets checked: `src`, `src-bugs`, `src-compliance`, `wolfcrypt-api_misuse`, `wolfcrypt-bugs`, `wolfcrypt-compliance`, `wolfcrypt-concurrency`, `wolfcrypt-portability`, `wolfcrypt-src`

No new issues found in the changed files. ✅

Frauschi force-pushed the `zd21457` branch 2 times, most recently from **`77407d5`** to **`559d88e`** last week

Compare

Frauschi assigned **wolfSSL-Bot** last week

douzzer commented last week — Contributor

only failing subtest is multi-test `all-c89-clang-tidy` "FAIL: scripts/ocsp-stapling2.test"

douzzer added Staged and removed Staged labels last week

douzzer requested changes last week

View reviewed changes

douzzer left a comment — Contributor

Missing some FIPS gating I suspect, re "Properly reject Ed448 identity public key"

```
[linuxkm-defaults-all-fips-v6-sanitizer] [35 of 52] [5a573e0c76]
    setting up FIPS "v6-linuxkm"...
    refreshing fips WCv6.0.0-linuxkm-UPDT-RC3... [caching link to git@github.com...
done]  done, now at 7756dbea90
    setting up FIPS "v6-linuxkm"...     refreshing wolfssl WCv6.0.0-linuxkm-UPDT-
RC2... done, now at b7220aeb4b
done [fips="WCv6.0.0-linuxkm-UPDT-RC3" (7756dbea90), wolfCrypt="WCv6.0.0-linuxkm-
UPDT-RC2" (def685129c)]
    configure with sanitizers...   real 0m10.090s  user 0m6.531s  sys 0m4.403s
    build...   real 0m38.522s  user 8m9.887s  sys 0m9.403s
    fixing FIPS hash in user library... done.
    check...FAIL: scripts/unit.test
   real 1m23.506s  user 2m1.463s  sys 0m15.917s
ERROR - tests/api.c line 6719 failed with:
    expected: wolfSSL_shutdown(ssl_c) == WOLFSSL_SUCCESS
    result:   2 != 1
ERROR - tests/api.c line 34781 failed with:
    expected: wc_ed448_import_public_fips(identity, sizeof(identity), &key) != 0
    result:   0 == 0
ERROR - tests/api.c line 36066 failed with:
    expected: Test failed
    result:   ret 0
   1306: test_pkcs7_decode_encrypted_outputsz              : skipped
   1307: test_pkcs7_ori_oversized_oid                      : skipped
   1308: test_wolfSSL_Cleanup                              : passed (  0.00001)

FAILURES:
   1305: test_ed448_rejects_identity_key

 End API Tests
```

```
 Failed/Skipped/Passed/All: 1/443/864/1308
FAIL scripts/unit.test (exit status: 1)

scripts/unit.log tail:
   1306: test_pkcs7_decode_encrypted_outputsz              : skipped
   1307: test_pkcs7_ori_oversized_oid                      : skipped
   1308: test_wolfSSL_Cleanup                              : passed (  0.00001)

FAILURES:
   1305: test_ed448_rejects_identity_key

 End API Tests
 Failed/Skipped/Passed/All: 1/443/864/1308
FAIL scripts/unit.test (exit status: 1)
    linuxkm-defaults-all-fips-v6-sanitizer fail_analytic_check
    failed config: 'EXTRA_CPPFLAGS=-Werror' '--srcdir' '.' '--disable-jobserver' '--
enable-option-checking=fatal' '--enable-fips=v6' '--enable-linuxkm-defaults' '--
enable-intelasm' '--enable-sp-asm' '--enable-all' '--enable-acert' '--enable-dtls13'
'--enable-dtls-mtu' '--enable-dtls-frag-ch' '--enable-dtlscid' '--enable-quic' '--
with-sys-crypto-policy' '--disable-srtp' 'CC=gcc-16' 'LDFLAGS=-g -fno-omit-frame-
pointer -fsanitize-recover=all -fsanitize=address,pointer-
subtract,leak,undefined,float-cast-overflow,float-divide-by-zero,bounds-strict -
fsanitize-recover=all ' 'CFLAGS=-DTEST_ALWAYS_RUN_TO_END -Wno-declaration-after-
statement -DDEBUG_LINUXKM_PIE_SUPPORT -DWC_SIPHASH_NO_ASM -DWC_DEBUG_CIPHER_LIFECYCLE
-g -fno-omit-frame-pointer -fsanitize=address,pointer-subtract,leak,undefined,float-
cast-overflow,float-divide-by-zero,bounds-strict -fsanitize-recover=all --param=max-
vartrack-size=128000000' 'CPPFLAGS=-DNO_WOLFSSL_CIPHER_SUITE_TEST -pedantic -Wnull-
dereference -Wdeclaration-after-statement'
```

Frauschi added 5 commits 5 days ago

fix for wc_DhAgree public key validation ···	50f28d9
Cap DTLS1.3 max ACK records to prevent overflow ···	cece804
Properly reject Ed448 identity public key ···	2237297
Respect outputSz in PKCS7 decode methods ···	1de4020
Fix stack buffer overflow in wc_PKCS7_DecryptOri ···	✕ 580cbe2

Frauschi force-pushed the `zd21457` branch from **559d88e** to **580cbe2** 5 days ago Compare

Frauschi commented 5 days ago Contributor Author

@douzzer I fixed the FIPS gating

Frauschi requested a review from **douzzer** 5 days ago

douzzer added the Staged label 3 days ago

douzzer approved these changes 3 days ago

View reviewed changes

douzzer merged commit **efe6ad4** into `wolfSSL:master` 3 days ago

494 of 497 checks passed

View details

Frauschi deleted the `zd21457` branch 3 days ago

JacobBarthelmeh mentioned this pull request 2 days ago

Various security fixes and tests #10088

Merged

Reviewers

wolfSSL-Fenrir-bot

douzzer

Assignees

wolfSSL-Bot

Labels

For This Release Staged

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants