

wolfSSL / wolfssl Public

<> Code Issues 17 Pull requests 92 Actions Projects Wiki Secu

Various fixes #10102

Merged douzzer merged 7 commits into wolfSSL:master from Frauschi:zd21460 3 days ago

Conversation Commits 7 Checks Files changed



Frauschi commented [last week](#)

Contributor

zd21460



Frauschi added the **For This Release** label [last week](#)



Frauschi force-pushed the `zd21460` branch 7 times, most recently from `9695426` to `a46a2f6`

[last week](#)

[Compare](#)



Frauschi self-assigned this [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 #10102

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

Findings: 1

1 finding(s) posted as inline comments (see file-level comments below)

This review was generated automatically by Fenrir. Findings are non-blocking.

wolfcrypt/src/ecc.c Outdated Show resolved

Frauschi force-pushed the `zd21460` branch from `0d8acd2` to `766ec21` last week Compare

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 #10102

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

Findings: 2

2 finding(s) posted as inline comments (see file-level comments below)

This review was generated automatically by Fenrir. Findings are non-blocking.

wolfcrypt/src/ecc.c Outdated Show resolved

wolfcrypt/src/aes.c Show resolved

Frauschi force-pushed the `zd21460` branch 2 times, most recently from `9f0c33c` to `2ab737b` last week Compare

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 #10102

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

Findings: 2

2 finding(s) posted as inline comments (see file-level comments below)

This review was generated automatically by Fenrir. Findings are non-blocking.

wolfcrypt/src/eccsi.c

Show resolved

wolfcrypt/src/ecc.c Outdated

Show resolved



Frauschi added 3 commits [last week](#)



CMAC: fix wraparound in streaming update. ...

[10953f0](#)



eccsi: fix universal signature forgery via r=0/s=0 ...

[13a0163](#)



evp: verify Poly1305 tag on ChaCha20-Poly1305 decrypt ...

[1fadd6](#)



Frauschi [force-pushed](#) the `zd21460` branch from `2ab737b` to `4c23d4d` [last week](#)

[Compare](#)



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 #10102

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 `zd21460` branch from `4c23d4d` to `e19f407` last week

[Compare](#)



Frauschi assigned **wolfSSL-Bot** and unassigned **Frauschi** last week

douzzaer commented last week

[Contributor](#)

only failing subtest is multi-test PRB `all-c89-clang-tidy` "FAIL: scripts/ocsp-stapling_tls13multi.test"



douzzaer added the `Staged` label last week



douzzaer requested changes last week

[View reviewed changes](#)



douzzaer left a comment

[Contributor](#)

"ecc: fix invalid-curve attack via missing on-curve validation" is causing an intolerable regression in ECC throughput:

```
benchmark-wolfcrypt-intelasm-sp-asm-all:
```

```
  3 asym alg(s) not fast enough in any trial:
```

```
  ECDHE[SECP256R1],256,agree -- best trial 49.27% of baseline, Z+1241.91
```

```
  ECC[SECP256R1],256,encrypt -- best trial 50.89% of baseline, Z+573.18
```

```
  ECC[SECP256R1],256,decrypt -- best trial 34.30% of baseline, Z+1831.97
```





We'll need to find a middle ground for validation that doesn't clobber performance.



douzzaer removed the `Staged` label last week

 **Frauschi** added 4 commits [last week](#)

-   [pkcs7,aes: reject truncated GCM auth tags](#) ... [a88dd07](#)
-   [x509: fix CA:FALSE bypass in wolfSSL_X509_verify_cert](#) ... [e5ab7fa](#)
-   [tls: fix ECH heap buffer overflow via publicName SNI pollution](#) ... [1823f2e](#)
-   [evp: fix EVP_PKEY2PKCS8 returning NULL for private-key-only EC keys](#) ...  [2ae2072](#)

  **JacobBarthelmeh** [force-pushed](#) the `zd21460` branch from `e19f407` to `2ae2072` [Compare](#)
[last week](#)

JacobBarthelmeh commented [last week](#) • edited ▾

Contributor

I removed one ECC commit due to a regression in performance that needs investigated farther. The other commits stayed exactly the same.

  **Frauschi** mentioned this pull request [5 days ago](#)

[Improved ECC curve validation #10133](#)

 Merged

Frauschi commented [5 days ago](#)

Contributor

Author

I created [#10133](#) with an updated version of the removed commit with the performance regression.

This one should now be ready to merge.

 1

  **Frauschi** requested a review from **douzer** [5 days ago](#)



JacobBarthelmeh approved these changes [3 days ago](#)

[View reviewed changes](#)



dgarske approved these changes [3 days ago](#)



View reviewed changes



douzer added the **Staged** label 3 days ago



douzer approved these changes 3 days ago

View reviewed changes



douzer merged commit **32502e9** into **wolfSSL:master** 3 days ago
495 of 496 checks passed

[View details](#)



Frauschi deleted the **zd21460** branch 3 days ago

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Reviewers



wolfSSL-Fenrir-bot



dgarske



douzer



JacobBarthelmeh



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

6 participants

