

New issue

[Jump to bottom](#)

# Remove WOLFSSL\_SESSION\_TYPE\_REF buffers from WOLFSSL\_SESSION #5476

 Merged

dgarske merged 4 commits into [wolfSSL:master](#) from [julek-wolfssl:session-buffers](#) 📄 on Aug 22

Conversation 17

Commits 4

Checks 3

Files changed 5



**julek-wolfssl** commented on Aug 17 • edited ▼

Member

ZD 14662

- Refactor ticket size to not accidentally go over WOLFSSL\_TICKET\_ENC\_SZ
  - Optimize memory usage. Write directly to ssl->session->ticket in CreateTicket() and use a hash to make sure the InternalTicket was encrypted.
  - DoClientTicket does not fatally error out anymore. Errors in the ticket result in the ticket being rejected instead.



**julek-wolfssl** self-assigned this on Aug 17



**julek-wolfssl** requested a review from **dgarske** 3 months ago



**dgarske** self-assigned this on Aug 17



Remove WOLFSSL\_SESSION\_TYPE\_REF buffers from WOLFSSL\_SESSION

✖ 68f71d0



**julek-wolfssl** force-pushed the `session-buffers` branch from `8f08a02` to `68f71d0`  
3 months ago

[Compare](#)

**dgarske** requested changes on Aug 17

[View changes](#)



**dgarske** left a comment

Contributor

@julek-wolfssl not sure if it is your PR changes, but this is consistently failing Jenkins:

```
./configure --enable-sp-math-all --enable-all --enable-intelasm --enable-sp-asm && make  
FAIL: scripts/unit.test
```



**dgarske** removed their assignment on Aug 17

**julek-wolfssl** commented on Aug 18

Member

Author

@**dgarske** The Jenkins issue was due to the size of the ticket object exceeding `ssl->session->staticTicket`. I'm not sure how my PR triggered that but I pushed a major overhaul to the ticket generation. I've made it more efficient and less error prone since the size is now calculated based on components and asserted to make sure everything fits where it should.

**dgarske** requested changes on Aug 18

[View changes](#)



**dgarske** left a comment

Contributor

Refactor looks good. Seems like a minor build macro issue...

```
[1;38;5;243m--enable-sslsv3 --enable-tls10 --enable-certgen --enable-certtext --enable-keygen --  
enable-testcert --enable-ecc --enable-supportedcurves --enable-curve25519 --enable-aesgcm --  
enable-camellia --enable-intelasm --enable-intelrand --disable-hashdrbg --enable-des3 --enable-  
ocspstapling --enable-ocspstapling2 --enable-certreq --enable-sha224 --enable-opensslextra --  
enable-psk --enable-sni --enable-alpn --enable-renegotiation-indication --enable-fpecc --disable-  
harden C_EXTRA_FLAGS="-DHAVE_FFDHE_2048 -DHAVE_FFDHE_3072 -DHAVE_FFDHE_4096 -DHAVE_FFDHE_6144 -  
DHAVE_FFDHE_8192 -D_MAX_CERTIFICATE_SZ=20000 -DWC_CTC_MAX_ALT_SIZE=20000 -DWOLFSSL_ALT_NAMES -  
DWOLFSSL_STATIC_RSA -DUSE_QAE_THREAD_LS -DWC_ASYNC_NO_AES -DWC_ASYNC_NO_HASH -DUSE_QAE_STATIC_MEM  
-DWC_NO_ASYNC_THREADING -DHAVE_IO_TIMEOUT -DDEFAULT_TIMEOUT_SEC=2 -DFP_ENTRIES=63 -DFP_LUT=12 -  
DWOLFSSL_ALWAYS_VERIFY_CB -DWOLFSSL_ALT_CERT_CHAINS -DWC_NO_CACHE_RESISTANT -DTFM_HUGE_SET -  
DWOLFSSL_NONBLOCK_OCSP -DHAVE_INTEL_MULX -mavx2 -mfma -fgnu89-inline"❖[0m
```



The case with `C_EXTRA_FLAGS` + double-quotes

```
EXTRACTED_CFLAGS = -DHAVE_FFDHE_2048 -DHAVE_FFDHE_3072 -DHAVE_FFDHE_4096 -DHAVE_FFDHE_6144 -  
DHAVE_FFDHE_8192 -D_MAX_CERTIFICATE_SZ=20000 -DWC_CTC_MAX_ALT_SIZE=20000 -DWOLFSSL_ALT_NAMES -  
DWOLFSSL_STATIC_RSA -DUSE_QAE_THREAD_LS -DWC_ASYNC_NO_AES -DWC_ASYNC_NO_HASH -DUSE_QAE_STATIC_MEM  
-DWC_NO_ASYNC_THREADING -DHAVE_IO_TIMEOUT -DDEFAULT_TIMEOUT_SEC=2 -DFP_ENTRIES=63 -DFP_LUT=12 -  
DWOLFSSL_ALWAYS_VERIFY_CB -DWOLFSSL_ALT_CERT_CHAINS -DWC_NO_CACHE_RESISTANT -DTFM_HUGE_SET -  
DWOLFSSL_NONBLOCK_OCSP -DHAVE_INTEL_MULX -mavx2 -mfma -fgnu89-inline
```

```
Testing CONFIG_REMAINDER = --enable-sslv3 --enable-tls10 --enable-certgen --enable-certtext --
enable-keygen --enable-testcert --enable-ecc --enable-supportedcurves --enable-curve25519 --
enable-aesgcm --enable-camellia --enable-intelasm --enable-intelrand --disable-hashdrbg --enable-
des3 --enable-ocspstapling --enable-ocspstapling2 --enable-certreq --enable-sha224 --enable-
opensslextra --enable-psk --enable-sni --enable-alpn --enable-renegotiation-indication --enable-
fpecc --disable-harden
[1;32mConfigure RESULT = 0[0m
```

```
make[2]: warning: -j9 forced in submake: resetting jobserver mode.
In file included from src/internal.c:89:
./wolfssl/internal.h:3671:5: error: unknown type name 'TicketNonce'
3671 |     TicketNonce     ticketNonce;    /* Nonce used to derive PSK */
      |     ^~~~~~
In file included from src/wolfio.c:37:
```

  Refactor ticket size to not accidentally go over WOLFSSL\_TICKET\_ENC\_SZ ... ✖ 4d0ea62


  **julek-wolfssl** force-pushed the session-buffers branch from d65476e to 4d0ea62 Compare  
3 months ago

julek-wolfssl commented on Aug 18 Member Author

I misunderstood when TicketNonce should be defined. Did && instead of || .


dgarske requested changes on Aug 18

[View changes](#)

 dgarske left a comment Contributor


I also verified async still works ( --enable-all --enable-asynccrypt ).

src/internal.c  Show resolved

src/internal.c  Show resolved

dgarske requested changes on Aug 18

[View changes](#)



 dgarske left a comment Contributor

Multi-test came up with an error:

```
[all-gcc-c99] [4 of 18] [802ff84160]
configure... real 0m16.293s user 0m11.224s sys 0m6.879s
build...In file included from src/internal.c:89:
src/internal.c: In function 'CreateTicket':
./wolfssl/internal.h:1710:18: error: redefinition of typedef '_args_test' [-Werror=pedantic]
1710 |     typedef char _args_test[sizeof((x)) >= sizeof((y)) ? 1 : -1];    \
      |             ^~~~~~
src/internal.c:33395:9: note: in expansion of macro 'WOLFSSL_ASSERT_SIZEOF_GE'
33395 |         WOLFSSL_ASSERT_SIZEOF_GE(et->enc_ticket, *it);
      |         ^~~~~~
./wolfssl/internal.h:1710:18: note: previous declaration of '_args_test' was here
1710 |     typedef char _args_test[sizeof((x)) >= sizeof((y)) ? 1 : -1];    \
      |             ^~~~~~
src/internal.c:33394:9: note: in expansion of macro 'WOLFSSL_ASSERT_SIZEOF_GE'
33394 |         WOLFSSL_ASSERT_SIZEOF_GE(ssl->session->staticTicket, *et);
      |         ^~~~~~
./wolfssl/internal.h:1710:5: error: ISO C90 forbids mixed declarations and code [-Werror=declaration-after-statement]
1710 |     typedef char _args_test[sizeof((x)) >= sizeof((y)) ? 1 : -1];    \
      |     ^~~~~~
src/internal.c:33395:9: note: in expansion of macro 'WOLFSSL_ASSERT_SIZEOF_GE'
33395 |         WOLFSSL_ASSERT_SIZEOF_GE(et->enc_ticket, *it);
      |         ^~~~~~
cc1: all warnings being treated as errors
make[2]: *** [Makefile:6176: src/libwolfssl_la-internal.lo] Error 1
```

  Fix avoidSysCalls logic

 06022e8

  julek-wolfssl assigned dgarske and unassigned julek-wolfssl on Aug 19

julek-wolfssl commented on Aug 19

Member

Author

Wrapped WOLFSSL\_ASSERT\_SIZEOF\_GE in a do..while to allow multiple uses in one function.

  julek-wolfssl requested a review from dgarske 3 months ago

dgarske requested changes on Aug 19

[View changes](#)

 dgarske left a comment

Contributor

Testing DEFAULT: --disable-inline

❖[1;32mConfigure RESULT = 0❖[0m

make[2]: warning: -j9 forced in submake: resetting jobserver mode.

wolfcrypt/src/misc.c:808:28: error: no previous prototype for ‘MakeWordFromHash’ [-Werror=missing-prototypes]

```
808 | WC_STATIC WC_INLINE word32 MakeWordFromHash(const byte* hashID)
    |                                     ^~~~~~
```

wolfcrypt/src/misc.c:821:28: error: no previous prototype for ‘HashObject’ [-Werror=missing-prototypes]

```
821 | WC_STATIC WC_INLINE word32 HashObject(const byte* o, word32 len, int* error)
    |                                     ^~~~~~
```

cc1: all warnings being treated as errors``

  **dgarske** assigned **julek-wolfssl** and unassigned **dgarske** on Aug 19

  Refactor and code review ...

✓ e565d0d

  **julek-wolfssl** force-pushed the `session-buffers` branch from **79e9ac3** to **e565d0d**  
3 months ago

[Compare](#)

  **dgarske** self-requested a review 3 months ago

  **dgarske** assigned **dgarske** and unassigned **julek-wolfssl** on Aug 22

**dgarske** requested changes on Aug 22

[View changes](#)

src/internal.c

33641	33554	}
33642	33555	
33643	33556	et = (ExternalTicket*)input;
33644	33557	
33645	33558	/* decrypt */
33646	-	ato32(et->enc_len, &inLen);
33647	-	if (inLen > (word16)(len - WOLFSSL_TICKET_FIXED_SZ)) {
	33559	+ ato16(et->enc_len, &inLen);



**dgarske** on Aug 22

**Contributor**

Please revert back to using 32-bit here! This was specifically changed to 32-bit to avoid an alignment padding issue. See [#4908](#)



**dgarske** on Aug 22

Contributor

Also please add an inline code comment to prevent this from changing again in the future. The structure element `enc_len` needs to be 32-bit aligned.



**dgarske** on Aug 22

Contributor

From [@julek-wolfssl](#) :

I disagree that this (referring to your last comment in 5476) needs to be reverted. I took a look at the original issue and the cause of the error was that in 5.2 the `InternalTicket` looked like this:

```
/* our ticket format */
typedef struct InternalTicket {
    ProtocolVersion pv;                /* version when ticket created */
    byte suite[SUITE_LEN];             /* cipher suite when created */
    byte msecret[SECRET_LEN];          /* master secret */
    word32 timestamp;                  /* born on */
    word16 haveEMS;                    /* have extended master secret */
#ifdef WOLFSSL_TLS13
    word32 ageAdd;                     /* Obfuscation of age */
    word16 namedGroup;                 /* Named group used */
    TicketNonce ticketNonce;          /* Ticket nonce */
#ifdef WOLFSSL_EARLY_DATA
    word32 maxEarlyDataSz;             /* Max size of early data */
#endif
#endif
} InternalTicket;
```

It has `word32` and `word16` members. I fixed this in [617eda9](#) by changing everything to byte buffers. I ran into the same issue described in 4887 and changing the struct over to byte arrays was the correct fix.



**dgarske** on Aug 22

Contributor

FYI: `enc_len` used to be `word16` , then we changed it to `word32` and now changing it back to `word16` .



**dgarske** assigned [julek-wolfssl](#) and unassigned **dgarske** on Aug 22

**dgarske** approved these changes on Aug 22

[View changes](#)



**dgarske** merged commit **b9d9dc0** into **wolfSSL:master** on Aug 22

27 checks passed

[View details](#)

---

#### Reviewers



**dgarske**



---

#### Assignees



**julek-wolfssl**

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

Successfully merging this pull request may close these issues.

None yet

---

#### 2 participants

