wolfSSL / **wolfssl** Public

Code Issues 38 **Pull requests 35** Actions Projects Wiki ...

New issue Jump to bottom

Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear #5468

Merged **cconlon** merged 1 commit into `wolfSSL:master` from `SparkiDev:wolfssl_clear` on Aug 17

Conversation 2 Commits 1 Checks 3 Files changed 5

SparkiDev commented on Aug 14 • edited by dgarske Contributor

Description

Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear. The `ssl->arrays` and `ssl->rng` fields (as well as a few options bits) needed to be cleared to enable this use-case.

Fixes ZD14659

Testing

Patched example server and client to use `wolfSSL_clear` :

```
diff --git a/examples/client/client.c b/examples/client/client.c
index 1d12aa6bf..152988d86 100644
--- a/examples/client/client.c
+++ b/examples/client/client.c
@@ -4190,12 +4190,20 @@ THREAD_RETURN WOLFSSL_THREAD client_test(void* args)
     wolfSSL_PrintStatsConn(&ssl_stats);
 #endif

-    wolfSSL_free(ssl); ssl = NULL;
+    if (!resumeSession) {
+        wolfSSL_free(ssl); ssl = NULL;
+    }
     CloseSocket(sockfd);

 #ifndef NO_SESSION_CACHE
     if (resumeSession) {
+    #if defined(OPENSSL_EXTRA) || defined(WOLFSSL_WPAS_SMALL)
+        /* test re-use of wolfSSL session via wolfSSL_clear */
+        wolfSSL_clear(ssl);
+        sslResume = ssl;
+    #else
         sslResume = wolfSSL_new(ctx);
+    #endif
         if (sslResume == NULL) {
             wolfSSL_CTX_free(ctx); ctx = NULL;
             err_sys("unable to get SSL object");
diff --git a/examples/server/server.c b/examples/server/server.c
index 049986b97..b1e4fcf18 100644
--- a/examples/server/server.c
+++ b/examples/server/server.c
@@ -2764,7 +2764,9 @@ THREAD_RETURN WOLFSSL_THREAD server_test(void* args)
         SetupPkCallbacks(ctx);
 #endif

-    ssl = SSL_new(ctx);
+    if (ssl == NULL) {
+        ssl = SSL_new(ctx);
+    }
     if (ssl == NULL)
         err_sys_ex(catastrophic, "unable to create an SSL object");

@@ -3515,7 +3517,13 @@ THREAD_RETURN WOLFSSL_THREAD server_test(void* args)
         wolfSSL_PrintStatsConn(&ssl_stats);

 #endif
+
+    #if defined(OPENSSL_EXTRA) || defined(WOLFSSL_WPAS_SMALL)
+        /* test re-use of wolfSSL session via wolfSSL_clear */
+        wolfSSL_clear(ssl);
+    #else
         SSL_free(ssl); ssl = NULL;
+    #endif

         CloseSocket(clientfd);

@@ -3531,6 +3539,8 @@ THREAD_RETURN WOLFSSL_THREAD server_test(void* args)
         }
     } /* while(1) */

+    SSL_free(ssl); ssl = NULL;
+
     WOLFSSL_TIME(cnt);
     (void)cnt;
```

Checklist

- □ added tests
- □ updated/added doxygen

□ updated appropriate READMEs
□ Updated manual and documentation

SparkiDev self-assigned this on Aug 14

dgarske assigned **dgarske** and unassigned **SparkiDev** on Aug 15

dgarske changed the title ~~wolfSSL_clear: fixups~~ **Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear** on Aug 15

dgarske force-pushed the `wolfssl_clear` branch from **`7c1a8cd`** to **`4f2acc3`** 3 months ago Compare

dgarske commented on Aug 15 Contributor

This is not ready: Need to review `--enable-asynccrypt` use case

And:

```
./examples/server/server -v 4 -l TLS13-AES128-GCM-SHA256 -r -2
./examples/client/client -v 4 -l TLS13-AES128-GCM-SHA256 -r -0 -2
```

dgarske force-pushed the `wolfssl_clear` branch from **`4f2acc3`** to **`b278fd7`** 3 months ago Compare

dgarske assigned **cconlon** on Aug 16

dgarske requested a review from **cconlon** 3 months ago

`Fixes to better handle re-use of a WOLFSSL object via wolfSSL_clear.` ✓ 7435402

dgarske force-pushed the `wolfssl_clear` branch from **`b278fd7`** to **`7435402`** 3 months ago Compare

dgarske removed their assignment on Aug 17

cconlon approved these changes on Aug 17

View changes

cconlon merged commit **91a49da** into `wolfSSL:master` on Aug 17

27 checks passed

View details

✓ **maxammann** approved these changes on Aug 18

View changes

maxammann left a comment

Looks good to me!

Reviewers

cconlon ✓

maxammann ✓

Assignees

cconlon

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants