RTI TLS Support

Release Notes

Version 7.0.0

Trademarks

RTI, Real-Time Innovations, Connext, NDDS, the RTI logo, 1RTI and the phrase, "Your Systems. Working as one," are registered trademarks, trademarks or service marks of Real-Time Innovations, Inc. All other trademarks belong to their respective owners.

Copy and Use Restrictions

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form (including electronic, mechanical, photocopy, and facsimile) without the prior written permission of Real-Time Innovations, Inc. The software described in this document is furnished solely under and subject to RTI's standard terms and conditions available at https://www.rti.com/terms and in accordance with your License Acknowledgement Certificate (LAC) and Maintenance and Support Certificate (MSC), except to the extent otherwise accepted in writing by a corporate officer of RTI.

This is an independent publication and is neither affiliated with, nor authorized, sponsored, or approved by, Microsoft Corporation.

The security features of this product include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Notices

Deprecations and Removals

Any deprecations or removals noted in this document serve as notice under the Real-Time Innovations, Inc. Maintenance Policy #4220 and/or any other agreements by and between RTI and customer regarding maintenance and support of RTI's software.

Deprecated means that the item is still supported in the release, but will be removed in a future release. *Removed* means that the item is discontinued or no longer supported. By specifying that an item is deprecated in a release, RTI hereby provides customer notice that RTI reserves the right after one year from the date of such release and, with or without further notice, to immediately terminate maintenance (including without limitation, providing updates and upgrades) for the item, and no longer support the item, in a future release.

Early Access Software

"Real-Time Innovations, Inc. ("RTI") licenses this Early Access release software ("Software") to you subject to your agreement to all of the following conditions:

(1) you may reproduce and execute the Software only for your internal business purposes, solely with other RTI software licensed to you by RTI under applicable agreements by and between you and RTI, and solely in a non-production environment;

(2) you acknowledge that the Software has not gone through all of RTI's standard commercial testing, and is not maintained by RTI's support team;

(3) the Software is provided to you on an "AS IS" basis, and RTI disclaims, to the maximum extent permitted by applicable law, all express and implied representations, warranties and guarantees, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, satisfactory quality, and non-infringement of third party rights;

(4) any such suggestions or ideas you provide regarding the Software (collectively , "Feedback"), may be used and exploited in any and every way by RTI (including without limitation, by granting sub-licenses), on a non-exclusive, perpetual, irrevocable, transferable, and worldwide basis, without any compensation, without any obligation to report on such use, and without any other restriction or obligation to you; and

(5) TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL RTI BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY OR PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR FOR LOST PROFITS, LOST DATA, LOST REPUTATION, OR COST OF COVER, REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING WITHOUT LIMITATION, NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, WHETHER ARISING OUT OF OR RELATING TO THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF RTI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES."

Technical Support
Real-Time Innovations, Inc.
232 E. Java Drive
Sunnyvale, CA 94089
Phone: (408) 990-7444
Email: support@rti.com
Website: https://support.rti.com/

Contents

Chapter 1 Supported Platforms

See the column for *TLS Support* in the table of [Supported Platforms for Compiler-Dependent Product, in the RTI Connext Core Libraries Release Notes](#). See the column for TLS.

Chapter 2 Compatibility

TLS Support is designed for use with the TCP transport that is included with *RTI Connext*. If you choose to use *TLS Support*, it must be installed on top of an existing *RTI Connext* installation with the same version number. It can only be used on architectures that support the TCP transport (see the *RTI Connext Core Libraries Platform Notes*).

TLS Support 7.0.0 is API-compatible with OpenSSL® versions 1.1.0 through 1.1.1n, not with versions earlier than OpenSSL 1.1.0. Note that *TLS Support* 7.0.0 has only been tested by RTI using OpenSSL 1.1.1n. If you need *TLS Support* 7.0.0 to run against older versions of OpenSSL, please contact support@rti.com.

TLS Support 7.0.0 uses TLS 1.3. When communicating with *TLS Support* 6.0.0 or below, *TLS Support* 7.0.0 uses TLS 1.1.

If you are upgrading from OpenSSL 1.0.1 to OpenSSL 1.0.2 or above: The number of bits of any Diffie-Hellman (DH) parameters must now be at least 1024 (see https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/). Therefore, if you are using the property **tls.cipher.dh_param_files** and there is a DH parameter file that has fewer than 1024 bits, you must regenerate the file with at least 1024 bits.

For backward-compatibility information between this and previous releases, see the *Migration Guide* on the RTI Community Portal (https://community.rti.com/documentation).

Chapter 3 What's Fixed in 7.0.0

3.1 Memory Leak when Running out of Memory

If either of the internal functions **RTITLS_ConnectionEndpointFactoryTLSv4_cre-ateConnectEndpoint()** or **RTITLS_ConnectionEndpointFactoryTLSv4_cre-ateAcceptEndpoint()** ran out of memory, connection creation would fail with a memory leak.

Here is one example set of error messages, along with a valgrind result:

```
NDDS_Transport_TCPv4_Plugin_clientOpenControlConnection_connEA:!create connection
endpoint
NDDS_Transport_TCPv4_Plugin_clientOpenControlConnection_connEA:error connecting to
peer at 127.0.0.1:36025
NDDS_Transport_TCPv4_Plugin_clientOpenControlConnection_connEA:failed to (re)connect
client control connection
NDDS_Transport_TCPv4_create_sendresource_srEA:failed to open client control
connection
==23757== 8,384 (6,280 direct, 2,104 indirect) bytes in 1 blocks are definitely lost
in loss record 128 of 134
==23757==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-
linux.so)
==23757==    by 0x13F366D: CRYPTO_malloc (mem.c:222)
==23757==    by 0x13F36A0: CRYPTO_zalloc (mem.c:230)
==23757==    by 0x1331070: SSL_new (ssl_lib.c:691)
==23757==    by 0xC0FDE9: RTITLS_ConnectionEndpointFactoryTLSv4_createConnectEndpoint
(TLSConnection.c:837)
==23757==    by 0x6266F8: NDDS_Transport_TCPv4_Plugin_clientOpenControlConnection_
connEA (Tcpv4.c:3321)
```

The leak would only happen if memory was already exhausted, so this problem did not lead to unbounded memory growth.

This problem has been fixed. Those two functions will now fail without a memory leak.

[RTI Issue ID COREPLG-589]

Chapter 4 Known Issues

Note: For an updated list of critical known issues, see the Critical Issues List on the RTI Customer Portal at https://support.rti.com.

4.1 Possible Valgrind still-reachable leaks when loading dynamic libraries

If you load any dynamic libraries, you may see "still reachable" memory leaks in "dlopen" and "dlclose". These leaks are a result of a bug in Valgrind (https://bugs.launchpad.net/ubuntu/+source/valgrind/+bug/1160352).

This issue affects the *Core Libraries*, *Security Plugins*, and *TLS Support*.

[RTI Issue IDs CORE-9941, SEC-1026, and COREPLG-510]