RTI Queuing Service

Release Notes

Version 6.1.1

Printed in U.S.A. First printing.
March 2022.

Trademarks

Copy and Use Restrictions

Notice

Any deprecations noted in this document serve as notice under the Real-Time Innovations, Inc. Maintenance Policy #4220.

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

1 Supported Platforms

RTI® Queuing Service is supported on the platforms in Table 1 Supported Platforms. For details on these platforms, see the *RTI Connext DDS Core Libraries Platform Notes*.

Table 1 Supported Platforms

Platform	Operating System
Linux®	All platforms on Intel® x64 CPUs listed in the *RTI Connext® DDSCore Libraries Release Notes* for the same version number, except SUSE® Linux Enterprise Server 12.
macOS®	All platforms on Intel x64 CPUs listed in the *RTI Connext DDS Core Libraries Release Notes* for the same version number.
Windows®	

Note: POSIX®-compliant architectures that end with "FACE_GP" are not supported. Custom target platforms are not supported.

2 Compatibility

Queuing Service is built on top of, and intended for use with, *RTI Connext® DDS* with the same version number.

For backward compatibility information, if any, between 6.1.1 and previous releases, see the *Migration Guide* on the RTI Community Portal (https://community.rti.com/documentation).

3 What's New in 6.1.1

3.1 Third-Party Software Upgrades

The following third-party software used by *Queuing Service* has been upgraded:

Third-Party Software	Previous Version	Current Version
SQLite® ODBC	0.9996	0.9998
SQLite	3.29.0	3.37.2
libxslt	1.1.29	1.1.34
libxml2	2.9.4	2.9.12
Bison	2.3	3.7.6
Flex	2.5.35	2.6.4

Some of these upgrades may fix potential vulnerabilities. See 4.2 Fixes Related to Vulnerabilities on page 4.

For information on third-party software used by *Connext DDS* products, see the "3rdPartySoftware" documents in your installation: **<NDDSHOME>/doc/manuals/connext_dds_professional/release_notes_3rdparty**.

4 What's Fixed in 6.1.1

4.1 RTICdrTypeCodeUtils_type_has_external_members:!get member error when running Queuing Service

The following, harmless error may have occurred when using *Queuing Service*:

```
RTICdrTypeCodeUtils_type_has_external_members:!get member
```

This problem has been fixed.

[RTI Issue ID QUEUEING-720]

4.2 Fixes Related to Vulnerabilities

This release fixes some potential vulnerabilities, described below.

4.2.1 Potential crash, leak of sensitive information, or service corruption upon XML parsing in Queuing Service due to vulnerabilities in libxml2

The *Queuing Service* XML parser had a third-party dependency on libxml2 version 2.9.4. That version of libxml2 is known to be affected by a number of publicly disclosed vulnerabilities.

These vulnerabilities have been fixed by upgrading to the latest stable version of libxml2, 2.9.12. See 3.1 Third-Party Software Upgrades on page 3.

The impact on *Queuing Service* of using the previous version varied depending on your *Queuing Service* configuration:

- With Connext Secure (enabling RTPS protection):
  - Exploitable through a compromised local file system containing a malicious XML file.

  - *Queuing Service* could crash or leak sensitive information. An attacker could compromise *Queuing Service* integrity.
  - CVSS v3.1 Score: 7.3 HIGH
  - CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

- Without Connext Secure (release mode):
  - Exploitable through a compromised local file system containing a malicious XML file.
  - Remotely exploitable through malicious RTPS messages.
  - *Queuing Service* could crash or leak sensitive information. An attacker could compromise *Queuing Service* integrity.
  - CVSS v3.1 Score: 8.6 HIGH
  - CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

- Without Connext Secure (debug mode):
  - Exploitable through a compromised local file system containing a malicious XML file.
  - Remotely exploitable through malicious RTPS messages.
  - *Queuing Service* could crash or leak sensitive information. An attacker could compromise *Queuing Service* integrity.
  - CVSS v3.1 Score: 9.8 CRITICAL
  - CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

[RTI Issue ID QUEUEING-734]

4.2.2 Potential arbitrary code execution upon parsing of a Sample Selector in Queueing Service due to vulnerabilities in Flex

The *Queuing Service* filter parser had a third-party dependency on Flex version 2.5.35. That version of Flex is known to be affected by a number of publicly disclosed vulnerabilities.

These vulnerabilities have been fixed by upgrading to the latest stable version of Flex, 2.6.4. See 3.1 Third-Party Software Upgrades on page 3.

The impact on *Queuing Service* of using the previous version varied depending on your *Queuing Service* configuration:

- With Connext Secure (enabling RTPS protection):
  - Exploitable through a compromised local file system containing an XML configuration file

with a malicious filter.

- *Queuing Service* could crash or leak sensitive information. An attacker could execute code with *Queuing Service* privileges.
- CVSS v3.1 Score: 8.4 HIGH
- CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- Without Connext Secure:
  - Exploitable through a compromised local file system containing an XML configuration file with a malicious filter.
  - Remotely exploitable through malicious RTPS messages.
  - *Queuing Service* could crash or leak sensitive information. An attacker could execute code with *Queuing Service* privileges.
  - CVSS v3.1 Score: 9.8 CRITICAL
  - CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

[RTI Issue ID QUEUEING-739]

4.2.3 Potential crash in Queuing Service due to multiple vulnerabilities in SQLite

Queuing Service had a third-party dependency on SQLite version 3.29.0. That version of SQLite is known to be affected by a number of publicly disclosed vulnerabilities.

These vulnerabilities have been fixed by upgrading to the latest stable version of SQLite, 3.37.2. See 3.1 Third-Party Software Upgrades on page 3.

The impact on *Queuing Service* of using the previous version varied depending on your *Queuing Service* configuration:

- With Connext Secure (enabling RTPS protection):
  - Exploitable through a compromised local file system containing malicious SQLite database files.
  - *Queuing Service* could crash.
  - CVSS v3.1 Score: 6.2 MEDIUM
  - CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- Without Connext Secure:
  - Exploitable through a compromised local file system containing malicious SQLite database

files.

- Remotely exploitable through malicious RTPS messages.
- *Queuing Service* could crash.
- CVSS v3.1 Score: 7.5 HIGH
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

[RTI Issue ID QUEUEING-741]

4.2.4 Potential crash, leak of sensitive information, or database corruption in Queuing Service due to multiple vulnerabilities in SQLite

This issue was fixed in 6.1.0, but not documented at that time.

In releases prior to 6.1.0, *Queuing Service* had a third-party dependency on SQLite version 3.7.2. That version of SQLite is known to be affected by a number of publicly disclosed vulnerabilities.

These vulnerabilities were fixed by upgrading to the latest stable version of SQLite, 3.29.0.

The impact on *Queuing Service* of using the previous version varied depending on your *Queuing Service* configuration:

- With Connext Secure (enabling RTPS protection):
  - Exploitable through a compromised local file system containing malicious SQLite database files.
  - *Queuing Service* could crash or leak sensitive information. An attacker could compromise Queueing Service integrity.
  - CVSS v3.1 Score: 5.9 MEDIUM
  - CVSS v3.1 Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
- Without Connext Secure:
  - Exploitable through a compromised local file system containing malicious SQLite database files.
  - Remotely exploitable through malicious RTPS messages.
  - *Queuing Service* could crash or leak sensitive information. An attacker could compromise Queueing Service integrity.
  - CVSS v3.1 Score: 7.3 HIGH
  - CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

[RTI Issue ID QUEUEING-743]

5 Previous Release

5.1 What's New in 6.1.0

5.1.1 New platforms

This release adds support for the following platforms:

- macOS 10.15 (x64)
- Red Hat® Enterprise Linux 7.6 (x64)
- Ubuntu® 20.04 LTS (x64)

5.1.2 Removed platforms

These platforms are no longer supported:

- 32-bit Linux and Windows platforms
- macOS 10.12
- Ubuntu 12.04 LTS

5.2 What's Fixed in 6.1.0

5.2.1 Potential crash, leak of sensitive information, or database corruption in Queuing Service due to multiple vulnerabilities in SQLite

See 4.2.4 Potential crash, leak of sensitive information, or database corruption in Queuing Service due to multiple vulnerabilities in SQLite on page 7 for details.

[RTI Issue ID QUEUEING-743]

6 Current Limitations

The QueueProducer and QueueConsumer wrapper APIs are only supported for the Modern C++ and .NET APIs.

7 Available Documentation

Queuing Service documentation also includes:

- **Getting Started Guide** (RTI_Queuing_Service_GettingStarted.pdf)—Provides installation and startup instructions.
- **User's Manual** (RTI_Queuing_Service_UsersManual.pdf)—Describes how to configure and use *Queuing Service*.