Introduction

This page provides a centralized resource for *RTI® Connext®* Security Bulletins and its previous Security Advisories publications. It presents a list of all *Connext* vulnerabilities that have been published through the CVE® Program.

If you believe you have found a vulnerability affecting RTI products, please report it to us by sending an email to security@rti.com.

RTI's Approach to Vulnerability Detection and Management

RTI considers vulnerabilities regardless of the source. We define a vulnerability as a product bug that affects the integrity or confidentiality of the system using our products, and can be triggered externally to the application. We follow industry practices, such as CVSS score, to assess the severity of vulnerabilities. Our software bill of materials (SBOM) (located in the *Connext* installation directory) details the third-party software included in RTI's products. Starting in *Connext Professional* 7.3.0, we provide the SBOM in CycloneDX and SPDX formats. When a vulnerability is reported in third-party software, RTI assesses its impact on RTI's products. RTI adds third-party vulnerabilities to its Security Bulletin when they directly affect its products. If a third-party vulnerability doesn't affect an RTI product, it's listed in a VEX document instead (see VEX Documents). This helps customers prioritize and manage third-party vulnerabilities more efficiently.

RTI applies best practices to detect vulnerabilities, including a secure coding standard, the use of static and dynamic analysis tools, fuzz testing, and long-running endurance tests.

RTI releases security patches for active LTS releases (see Connext Releases). We proactively create patches for most commonly used architectures in LTS releases. Customers can request patches for other architectures by contacting RTI Support (see the RTI Customer Portal). We include fixes to critical vulnerabilities in third-party software once a patch is available by the provider that is compatible with the version used in RTI's software.

RTI software distribution through the RTI Customer Portal includes a SHA-256 hash. Releases starting in 2024 are signed.

RTI communicates through its Security Bulletins the availability of new security patches and shares sufficient details (such as CVSS score/vector and mitigation options) about the fixes to enable RTI customers to do their own risk analysis.

VEX Documents

RTI provides VEX (Vulnerability Exploitability eXchange) documents to help customers understand the exploitability of third-party vulnerabilities in RTI products. They provide information on whether a vulnerability affects RTI products, the status of the vulnerability, and any applicable mitigations. These documents follow the recommendations from CISA's Minimum Requirements for VEX and use the CycloneDX VEX format.

We recommend our customers include these VEX documents as part of their own Software Composition Analysis. The following VEX documents are available for RTI products:

General VEX documents

Product	VEX File
Connext Professional	Download
Connext Micro	Download
Connext Cert	Download

Note

VEX files are updated regularly, and the links above always provide the latest versions. In each of our Security Bulletins, we publish specific VEX documents for the latest releases of our active LTS products. The VEX files published in each Security Bulletin are those generated at the time of the release; they are provided for convenience and are never updated afterwards. If you do not find your exact *Connext* version on these Security Bulletins, you can always use the general VEX documents, which include our latest assessment of the vulnerabilities. For the most up-to-date information on third-party vulnerabilities, please refer to the general VEX files above rather than the static VEX files included in the Security Bulletins.

Security Bulletins

The security and integrity of the systems built using the *Connext* products are of the utmost importance to us. We periodically inform you of any newly identified vulnerabilities in our software.

This section contains RTI Security Bulletins, our official communication channel for disclosing vulnerabilities that may affect RTI software. Each bulletin is assigned a unique identifier in the format `RTI-SB-<YYYY>-<MM>`, indicating the publication date. Bulletins include a list of CVEs related to vulnerabilities found either in RTI products or in their dependencies. Because CVE publication is asynchronous, a bulletin may reference CVEs originally published in a previous year (for example, `RTI-SB-2025-05` may include CVEs from 2024).

Release versions affected by the vulnerabilities are indicated using the following nomenclature: `"Affected: [FIRST AFFECTED VERSION] before [FIRST VERSION NOT AFFECTED]"`.

For example in the *"Affected RTI Connext Professional Releases"* section:

- *"Affected: 7.0.0 before 7.3.0.5"* means the vulnerability affects all *Connext Professional* versions starting from (and including) 7.0.0 until (and not including) 7.3.0.5.
- The * in an upper bound denotes "infinity", not a wildcard pattern. For example, *"Affected: 7.4.0 before 7.*"* means the associated vulnerability affects all *Connext Professional* 7.x version series starting with 7.4.0.

To take advantage of these vulnerabilities, the malicious user needs to be part of the network where *Connext* applications are actively running, or have access to the filesystem. When exploited, the *Connext* application may crash (potentially affecting confidentiality/integrity of the *Connext* application), or the attacker may execute code remotely with system privileges and/or gain unauthorized access to the contents of the memory owned by the *Connext* application.

To protect your *Connext* applications, consider these best practices:

1. Protect the network where *Connext* applications are running so untrusted peers cannot inject malicious RTPS or authentication messages.
2. Protect the file system *Connext* is accessing so untrusted peers cannot inject malicious modifications to configuration or database files.

Security patches are proactively available according to Maintenance Releases and Security Updates Policy. Please refer to individual Security Bulletins to see which patches are available. Patches for other long-term support versions of *Connext* will be made available upon request. For issues related to third-party software, fixes are subject to availability of a patch for the affected third-party software on the same major version currently used by that *Connext* version. Please contact support@rti.com to arrange for a patch on other versions and architectures, or if you do not see the patch listed in the portal. The RTI Support team will work with you on the patch plan and timeline. Please specify the version of the software, architecture, and an indication of the timeline.

RTI-SB-2026-03

Products and versions affected

- *RTI® Connext®* Professional Versions affected: 4.3x before 7.7.0
- *RTI® Connext®* Micro Versions affected: 4.0.0 before 4.3.0

Newly identified vulnerabilities

RTI has recently identified several new vulnerabilities, and a fix is available to address all the vulnerabilities. Type of issues:

- CWE-121: Stack-based Buffer Overflow
- CWE-125: Out-of-bounds Read
- CWE-126: Buffer Over-read
- CWE-297: Improper Validation of Certificate with Host Mismatch
- CWE-405: Asymmetric Resource Consumption (Amplification)
- CWE-476: NULL Pointer Dereference
- CWE-611: Improper Restriction of XML External Entity Reference
- CWE-754: Improper Check for Unusual or Exceptional Conditions
- CWE-770: Allocation of Resources Without Limits or Throttling
- CWE-787: Out-of-bounds Write

This is a detailed list of the issues included in this Security Bulletin, in spreadsheet format, for your convenience.

Available patches and best practices

A patch for long-term support versions of *Connext* is available on the RTI Customer Portal:

- *Connext Professional* 7.3.1.2 for 7.3.1

Please contact support@rti.com to arrange for a patch on other versions and architectures, or if you do not see the patch listed in the portal.

In addition to the patches mentioned above, the fixes in this Security Bulletin will be included in *Connext Professional* 7.7.0. and *Connext Micro* 4.3.0.

VEX document snapshots for this Security Bulletin

If your *Connext* version is different than these, then use the general VEX documents above, which include our latest assessment of third-party-related vulnerabilities.

Product	VEX File
Connext Professional 7.3.1.2	Download

CVE-2026-22796

[Critical] Potential Denial of Service in RTI Security Plugins for OpenSSL when parsing Permissions Document

The *RTI Security Plugins* depended on OpenSSL 3.5.1, which is known to be affected by the CVE-2026-22796 publicly disclosed vulnerability.

This vulnerability has been fixed by upgrading OpenSSL to the latest stable version, 3.5.5.

User Impact without Security

Not applicable (affects a security-specific product/feature only).

User Impact with Security

- Exploitable invalid or NULL pointer dereference in the *RTI Security Plugins* when parsing a Permissions Document.
- CVSS v3.1 Base Score: 7.5 High
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS 4.0 Base Score: 8.7 High
- CVSS 4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

There are no mitigations for this vulnerability.

CWE Classification

- `CWE-754`

CAPEC Classification

- `CAPEC-153`

Associated Issue IDs

- [CVE Issue ID CVE-2026-22796]
- [RTI Issue ID SEC-2893]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

CVE-2026-22795

[Critical] Potential Denial of Service in RTI Security Plugins for OpenSSL when loading Private Key

The *RTI Security Plugins* depended on OpenSSL 3.5.1, which is known to be affected by the CVE-2026-22795 publicly disclosed vulnerability.

This vulnerability has been fixed by upgrading OpenSSL to the latest stable version, 3.5.5.

User Impact without Security

Not applicable (affects a security-specific product/feature only).

User Impact with Security

- Exploitable invalid or NULL pointer dereference in the *RTI Security Plugins* when loading a private key.
- CVSS v3.1 Base Score: 5.5 Medium
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
- CVSS 4.0 Base Score: 6.7 Medium
- CVSS 4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

Protect access to the file system from which *Connext* applications are loading private keys.

CWE Classification

- `CWE-754`

CAPEC Classification

- `CAPEC-153`

Associated Issue IDs

- [CVE Issue ID CVE-2026-22795]
- [RTI Issue ID SEC-2895]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

CVE-2026-4374

[Critical] Potential unauthorized local file system read in Cloud Discovery Service when parsing a malicious XML configuration document

Improper restriction of an XML external entity reference vulnerability in Cloud Discovery Service when parsing a malicious XML configuration document could allow unauthorized local file system read access and Data Serialization External Entities Blowup.

User Impact without Security

A vulnerability in Cloud Discovery Service while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 7.7 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which Connext applications are loading XML QoS documents.

CWE Classification

- `CWE-611`

CAPEC Classification

- `CAPEC-201`, `CAPEC-221`

Associated Issue IDs

- [CVE Issue ID CVE-2026-4374]
- [RTI Issue ID CDS-280]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

[Critical] Potential unauthorized local file system read in Collector Service when parsing a malicious XML configuration document

Improper restriction of an XML external entity reference vulnerability in *Collector Service* when parsing a malicious XML configuration document could allow unauthorized local file system read access and Data Serialization External Entities Blowup.

User Impact without Security

A vulnerability in *Collector Service* while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 7.7 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which Connext applications are loading XML QoS documents.

CWE Classification

- `CWE-611`

CAPEC Classification

- `CAPEC-201`, `CAPEC-221`

Associated Issue IDs

- [CVE Issue ID CVE-2026-4374]
- [RTI Issue ID OCA-457]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.1.0 before 7.3.1.1

[Critical] Potential unauthorized local file system read in Queuing Service when parsing a malicious XML configuration document

Improper restriction of an XML external entity reference vulnerability in *Queuing Service* when parsing a malicious XML configuration document could allow unauthorized local file system read access and Data Serialization External Entities Blowup.

User Impact without Security

A vulnerability in *Queuing Service* while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 7.7 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which Connext applications are loading XML QoS documents.

CWE Classification

- `CWE-611`

CAPEC Classification

- `CAPEC-201`, `CAPEC-221`

Associated Issue IDs

- [CVE Issue ID CVE-2026-4374]
- [RTI Issue ID QUEUEING-798]

Affected RTI Connext Professional Releases

- Affected: 5.3.1 before 5.3.*

[Critical] Potential unauthorized local file system read in Recording Service when parsing a malicious XML configuration document

Improper restriction of an XML external entity reference vulnerability in *Recording Service* when parsing a malicious XML configuration document could allow unauthorized local file system read access and Data Serialization External Entities Blowup.

User Impact without Security

A vulnerability in *Recording Service* while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 7.7 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which Connext applications are loading XML QoS documents.

CWE Classification

- `CWE-611`

CAPEC Classification

- `CAPEC-201`, `CAPEC-221`

Associated Issue IDs

- [CVE Issue ID CVE-2026-4374]
- [RTI Issue ID RECORD-1571]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*

[Critical] Potential unauthorized local file system read in Routing Service when parsing a malicious XML configuration document

Improper restriction of an XML external entity reference vulnerability in *Routing Service* when parsing a malicious XML configuration document could allow unauthorized local file system read access and Data Serialization External Entities Blowup.

User Impact without Security

A vulnerability in Routing Service while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- Exploitable by providing malicious XML remotely through remote administration commands.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 8.8 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Routing Service* while loading configurations via XML could have resulted in the following:

- Unauthorized local file system read when parsing a malicious XML file.
- Availability of the service affected (denial of service) when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 7.7 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

CWE Classification

- `CWE-611`

CAPEC Classification

- `CAPEC-201`, `CAPEC-221`

Associated Issue IDs

- [CVE Issue ID CVE-2026-4374]
- [RTI Issue ID ROUTING-1353]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

CVE-2026-2394

[Critical] Potential heap buffer read overflow in Connext applications when parsing an XML type

There was a possible heap buffer overread of one byte when parsing an XML type.

User Impact without Security

This vulnerability could have caused the following on any application using XML types:

- Heap buffer overread of one byte leading to a small impact on confidentiality and a low probability of a crash.
- Exploitable through malicious RTPS messages.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 6.5 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
- CVSS v4.0 Base Score: 6.3 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could have caused the following on any application using XML types:

- Heap buffer overread of one byte leading to a small impact on confidentiality and a low probability of a crash.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 4.4 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L
- CVSS v4.0 Base Score: 4.8 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N

Mitigations

- Restrict permissions for writing to *Connext* XML type files, to prevent the Local Attack Vector, AND
- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector. Alternatively, enable *Security Plugins* endpoint discovery protection by setting `discovery_protection_kind` to a value other than NONE and setting `enable_discovery_protection` to TRUE in your Governance Document.

CWE Classification

- `CWE-126`

CAPEC Classification

- `CAPEC-540`

Associated Issue IDs

- [CVE Issue ID CVE-2026-2394]

- [RTI Issue ID CORE-16494]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 4.3x before 5.2.*

CVE-2025-68161

[Minor] Potential man-in-the-middle attack in Micro Application Generator when using Socket Appender in Apache Log4j™

The logging system in *Micro Application Generator* (MAG) could be configured to employ the Socket Appender in Apache Log4j, which is affected by the vulnerability CVE-2025-68161.

This vulnerability has been fixed by upgrading Apache Log4j to version 2.25.3.

User Impact without Security

The associated CVE could be exploited by manipulating files in the *Connext Micro* installation.

- CVSS v3.1 Score: 4.0 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
- CVSS v4.0 Score: 2.1 LOW
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:L/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect the directory where Connext is installed from modifications by unauthorized users.

CWE Classification

- `CWE-297`

CAPEC Classification

- `CAPEC-217`

Associated Issue IDs

- [CVE Issue ID CVE-2025-68161]
- [RTI Issue ID MAG-247]

Affected RTI Connext Micro Releases

- Affected: 4.0.0 before 4.3.0

CVE-2025-59375

[Critical] Potential Denial of Service in Connext applications when parsing XML files

Earlier releases of *Connext* depended on Expat 2.7.1, which is known to be affected by CVE-2025-59375, a publicly disclosed vulnerability. Release 7.7.0 uses a newer version of Expat that does not have this vulnerability.

User Impact without Security

This vulnerability could have resulted in the following:

- Large dynamic memory allocations when parsing a maliciously crafted small document.
- Exploitable through a compromised local file system containing malicious XML/DTD files.
- Remotely exploitable through malicious RTPS messages.
- CVSS v3.1 Score: 7.5 High
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Score: 8.7 High
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could have resulted in the following:

- Large dynamic memory allocations when parsing a maliciously crafted small document.
- Exploitable through a compromised local file system containing malicious XML/DTD files.
- CVSS v3.1 Score: 6.2 Medium
- CVSS v3.1 Vector:CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Score: 6.9 Medium
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files your *Connext* application uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-770`

CAPEC Classification

- `CAPEC-130`

Associated Issue IDs

- [CVE Issue ID CVE-2025-59375]
- [RTI Issue ID CORE-16200]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.2.29
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 4.4d before 5.2.*

CVE-2025-11187

[Critical] Potential stack buffer overflow in RTI Security Plugins for OpenSSL when loading Private Key

The *RTI Security Plugins* depended on OpenSSL 3.5.1, which is known to be affected by the CVE-2025-11187 publicly disclosed vulnerability.

This vulnerability has been fixed by upgrading OpenSSL to the latest stable version, 3.5.5.

User Impact without Security

Not applicable (affects a security-specific product/feature only).

User Impact with Security

- Exploitable stack buffer overflow in the *RTI Security Plugins* when loading a private key.
- CVSS v3.1 Base Score: 6.1 Medium
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:H
- CVSS 4.0 Base Score: 5.2 Medium

- CVSS 4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N

Mitigations

Protect access to the file system from which *Connext* applications are loading private keys.

CWE Classification

- `CWE-476`, `CWE-787`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2025-11187]
- [RTI Issue ID SEC-2894]

Affected RTI Connext Professional Releases

- Affected: 7.6.0 before 7.7.0
- Affected: 7.3.1 before 7.3.1.1
- Affected: 6.1.2.29 before 6.1.*

CVE-2025-9232

[Critical] Potential Denial of Service in RTI Security Plugins for OpenSSL when configuring client proxy

The *RTI Security Plugins* depended on OpenSSL 3.5.1, which is known to be affected by the CVE-2025-9232 publicly disclosed vulnerability.

This vulnerability has been fixed by upgrading OpenSSL to the latest stable version, 3.5.5.

User Impact without Security

Not applicable (affects a security-specific product/feature only).

User Impact with Security

- Exploitable Denial of Service in the *RTI Security Plugins* when the URL of the *DomainParticipant's* OCSP responder has an IPv6 address and you configure a client proxy through the `no_proxy` and `http_proxy` (or `https_proxy`) environment variables. Note that the *RTI Security Plugins* do not support configuring a client proxy for OCSP responders.
- CVSS v3.1 Base Score: 5.9 Medium

- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS 4.0 Base Score: 8.2 High
- CVSS 4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

Do not configure a client proxy when using the OCSP feature of the Security Plugins.

CWE Classification

- `CWE-125`

CAPEC Classification

- `CAPEC-540`

Associated Issue IDs

- [CVE Issue ID CVE-2025-9232]
- [RTI Issue ID SEC-2823]

Affected RTI Connext Professional Releases

- Affected: 7.6.0 before 7.7.0
- Affected: 7.3.1 before 7.3.1.1

CVE-2025-6021

[Critical] Potential stack buffer overflow in Cloud Discovery Service when parsing malicious XML

RTI Cloud Discovery Service could have been affected by a vulnerability found in the `Libxml2` third-party library. This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What's New.

User Impact without Security

A vulnerability in *Cloud Discovery Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector:` <https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L>`__CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID CDS-278]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

[Critical] Potential stack buffer overflow in Collector Service when parsing malicious XML

Collector Service could have been affected by a vulnerability found in the `Libxml2` third-party library (`rtixml2` in *Connext*). This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What’s New.

User Impact without Security

A vulnerability in the `rtixml2` library could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM

- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID OCA-452]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.1.0 before 7.3.1.1

[Critical] Potential stack buffer overflow in Queuing Service when parsing malicious XML

Queuing Service could have been affected by a vulnerability found in the `Libxml2` third-party library. This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What’s New.

User Impact without Security

A vulnerability in *Queuing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- Exploitable by providing malicious XML remotely through remote administration commands.
- CVSS v3.1 Base Score: 7.5 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 8.7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability *Queuing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

- Protect access to the file system from which *Connext* applications are loading XML QoS documents.
- Apply DDS security to *Routing Service* remote administration topics.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID QUEUEING-795]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 5.2.0 before 5.2.*

[Critical] Potential stack buffer overflow in Recording Service when parsing malicious XML

Recording Service could have been affected by a vulnerability found in the `Libxml2` third-party library. This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What's New.

User Impact without Security

A vulnerability in *Recording Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID RECORD-1566]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*

[Critical] Potential stack buffer overflow in library rtixml2 when parsing malicious XML

RTI’s `rtixml2` library could have been affected by a vulnerability found in the `Libxml2` third-party library. This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What’s New.

User Impact without Security

A vulnerability in the `rtixml2` library could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.

- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in "User Impact without Security" above.

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID ROUTING-1352]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

[Critical] Potential stack buffer overflow in Routing Service when parsing malicious XML

Routing Service could have been affected by a vulnerability found in the `Libxml2` third-party library. This issue has been resolved by upgrading to a newer version of the third-party library. See the third-party software upgrades in What's New.

User Impact without Security

A vulnerability in *Routing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- Exploitable by providing malicious XML remotely through remote administration commands.

- CVSS v3.1 Base Score: 7.5 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 8.7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Routing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.2 LOW
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

Protect access to the file system from which *Connext* applications are loading XML QoS documents.

Apply DDS security to *Routing Service* remote administration topics.

CWE Classification

- `CWE-121`, `CWE-787`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6021]
- [RTI Issue ID ROUTING-1362]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1.1
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*

CVE-2024-45590

[Major] Potential Denial of Service in System Designer when parsing the body of malicious HTTP requests

System Designer depended on *express* third-party software that required *body-parser 1.20.2*, which is known to be affected by the CVE-2024-45590 publicly disclosed vulnerability.

This vulnerability has been fixed by forcing *express* to get the latest stable version of body-parser, 1.20.3.

User Impact without Security

This vulnerability could have resulted in the following:

- Exploitable Denial of Service in *System Designer* when processing malicious HTTP requests that have URL encoding enabled.
- CVSS v3.1 Score: 7.5 HIGH.
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Score: 7.7 HIGH.
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:P

User Impact with Security

Same impact as described in “User Impact without Security” above

Mitigations

None

CWE Classification

- `CWE-405`

CAPEC Classification

- `CAPEC-130`

Associated Issue IDs

- [CVE Issue ID CVE-2024-45590]
- [RTI Issue ID SYSD-1420]

Affected RTI Connext Professional Releases

- Affected: 7.3.1 before 7.3.1.1
- Affected: 6.1.2 before 6.1.*

RTI-SB-2025-12

Products and versions affected

- *RTI® Connext®* Professional Versions affected: 6.1.0 to 7.6.0

Newly identified vulnerabilities

RTI has recently identified several new vulnerabilities, and a fix is available to address all the vulnerabilities. Type of issues:

- CWE-125: Out-of-Bounds Read
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor
- CWE-400: Uncontrolled Resource Consumption

This is a detailed list of the issues included in this Security Bulletin, in spreadsheet format, for your convenience.

Available patches and best practices

There is no patch release needed since fixes for the vulnerabilities mentioned in this security bulletin are available in *Connext Professional* 7.3.1. Please contact support@rti.com to arrange for a patch on other versions.

VEX document snapshots for this Security Bulletin

If your *Connext* version is different than 7.3.1.0, then use the general VEX documents above, which include our latest assessment of third-party-related vulnerabilities.

Product	VEX File
Connext Professional 7.3.1.0	Download

CVE-2025-10450

[Critical] Potential unauthorized access to instance information in Connext applications

An unauthorized access to instance information in *Connext* applications could have occurred while setting DDS_ReliabilityQosPolicy::instance_state_consistency_kind to DDS_RECOVER_INSTANCE_STATE_CONSISTENCY on a *DataReader*.

User Impact without Security

A vulnerability in *Connext* applications while enabling instance state consistency on a *DataReader* could have resulted in the following:

- Unauthorized access to limited information about instances (for example, how many alive and disposed instances a *DataWriter* has). This information does not include the serialized payloads of any samples.
- Remotely exploitable.
- Potential impact on the confidentiality, integrity, and availability of *Connext* applications.
- CVSS v3.1 Base Score: 8.6 High
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L
- CVSS v4.0 Base Score: 8.3 High
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Connext* applications while enabling instance state consistency on a *DataReader* could have resulted in the following:

- Unauthorized access to limited information about instances (for example, how many alive and disposed instances a *DataWriter* has). This information does not include the serialized payloads of any samples.
- Remotely exploitable.
- Potential impact on the confidentiality, integrity, and availability of *Connext* applications.
- CVSS v3.1 Base Score: 6.4 Medium
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L
- CVSS v4.0 Base Score: 6.1 Medium
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

Mitigations

There are no mitigations for this vulnerability.

CWE Classification

- `CWE-359`

CAPEC Classification

- `CAPEC-158`

Associated Issue IDs

- [CVE Issue ID CVE-2025-10450]
- [RTI Issue ID CORE-16119]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.2.0 before 7.3.1

CVE-2025-9086

[Critical] Potential crash in Collector Service when processing a malicious Set-Cookie header in an HTTP response

Collector Service had a third-party dependency on Curl 8.6.0, which is known to be affected by a number of publicly disclosed vulnerabilities. These vulnerabilities have been fixed by upgrading Curl to the latest stable version, 8.16.0.

User Impact without Security

This vulnerability in *Collector Service* could have resulted in the following:

- Exploitable by sending a malicious HTTP response.
- *Collector Service* could crash.
- CVSS v3.1 Base Score: 7.5 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- CVSS v4.0 Base Score: 8.7 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Avoid using *http://* for cookies.

CWE Classification

- `CWE-125`

CAPEC Classification

- `CAPEC-540`

Associated Issue IDs

- [CVE Issue ID CVE-2025-9086]
- [RTI Issue ID OCA-442]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.2.0 before 7.3.1

CVE-2025-5889

[Trivial] Potential Denial of Service in System Designer when parsing specific HTTP requests

System Designer depended on brace-expansion 1.1.11, which is known to be affected by the CVE-2025-5889 publicly disclosed vulnerability.

This vulnerability has been fixed by upgrading brace-expansion to the latest stable version, 1.1.12.

User Impact without Security

This vulnerability could have resulted in the following:

- Exploitable Denial of Service in System Designer when processing HTTP requests that lead to inefficient regular expression complexity.
- CVSS v3.1 Score: 3.1 LOW.
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
- CVSS v4.0 Score: 2.3 LOW.
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Avoid using the parameter `-all` when calling the `rtisystemdesigner` script. This limits the vector attack to requests coming from localhost.

CWE Classification

- `CWE-400`

CAPEC Classification

- `CAPEC-492`

Associated Issue IDs

- [CVE Issue ID CVE-2025-5889]
- [RTI Issue ID SYSD-1413]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.7.0
- Affected: 7.0.0 before 7.3.1
- Affected: 6.1.0 before 6.1.*

RTI-SB-2025-09

Products and versions affected

- *RTI® Connext®* Professional Versions affected: 4.x to 7.5.0

Newly identified vulnerabilities

RTI has recently identified several new vulnerabilities, and a fix is available to address all the vulnerabilities. Type of issues:

- CWE-122: Heap-Based Buffer Overflow
- CWE-125: Out-of-Bounds Read
- CWE-126: Buffer Over-read
- CWE-190: Integer Overflow or Wraparound
- CWE-193: Off-by-one Error
- CWE-197: Numeric Truncation Error
- CWE-416: Use After Free
- CWE-822: Untrusted Pointer Dereference
- CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')

This is a detailed list of the issues included in this Security Bulletin, in spreadsheet format, for your convenience.

Available patches and best practices

A patch for long-term support versions of *Connext* is available on the RTI Customer Portal:

- *Connext Professional* 7.3.0.10 for 7.3.0

Please contact support@rti.com to arrange for a patch on other versions and architectures, or if you do not see the patch listed in the portal.

In addition to the patches mentioned above, the fixes in this Security Bulletin will be included in *Connext Professional* 7.3.1 and *Connext Professional* 7.6.0.

VEX document snapshots for this Security Bulletin

If your *Connext* version is different than these, then use the general VEX documents above, which include our latest assessment of third-party-related vulnerabilities.

Product	VEX File
Connext Professional 7.3.0.10	Download

CVE-2025-7458

[Critical] Potential out-of-bounds read in RTI Recording Service during its initialization

An out-of-bounds read in *Recording Service* could have occurred during its initialization.

User Impact without Security

A vulnerability in *Recording Service* while initializing could have resulted in the following:

- Out-of-bounds read while executing a malicious SQLite statement.
- Exploitable by providing a malicious XML document to Recording Service during startup. Not remotely exploitable.
- Potential impact on the confidentiality of *Recording Service*.
- Potential crash in *Recording Service*.
- CVSS v3.1 Base Score: 7.7 High
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 6.9 Medium
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the local file system where *Recording Service* is going to store data.

CWE Classification

- `CWE-125`, `CWE-190`

CAPEC Classification

- `CAPEC-540`, `CAPEC-92`

Associated Issue IDs

- [CVE Issue ID CVE-2025-7458]
- [RTI Issue ID RECORD-1546]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.0.10
- Affected: 6.1.0 before 6.1.2.27
- Affected: 6.0.0 before 6.0.1.43

CVE-2025-3277

[Critical] Potential arbitrary code execution in RTI Recording Service during its initialization

An arbitrary code execution in *Recording Service* could have occurred during its initialization.

User Impact without Security

A vulnerability in *Recording Service* while initializing could have resulted in the following:

- Arbitrary code execution while executing a malicious SQLite statement.
- Exploitable by providing a malicious XML document to Recording Service during startup. Not remotely exploitable.
- Potential impact on the integrity and confidentiality of *Recording Service*.
- Potential crash in *Recording Service*.
- CVSS v3.1 Base Score: 8.4 High
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS v4.0 Base Score: 8.6 High
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the local file system where *Recording Service* is going to store data.

CWE Classification

- `CWE-122`, `CWE-190`

CAPEC Classification

- `CAPEC-100`, `CAPEC-92`

Associated Issue IDs

- [CVE Issue ID CVE-2025-3277]
- [RTI Issue ID RECORD-1545]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.0.10
- Affected: 6.1.0 before 6.1.2.27
- Affected: 6.0.0 before 6.0.1.43

CVE-2025-8410

[Critical] Potential heap buffer read overflow in Security Plugins when using a malicious identity certificate file

An out-of-bounds read on the heap could have occurred while processing a malicious identity certificate file. This problem did not affect the *Security Plugins* for wolfSSL.

User Impact without Security

Not applicable (affects a security-specific product/feature only).

User Impact with Security

A vulnerability in the *Connext* application could have resulted in the following:

- Heap buffer overread while processing a malicious identity certificate file.
- Exploitable by overwriting the identity certificate file on the file system with a malicious identity certificate file.
- Exploitable only when a race condition was won.

- Potential impact on confidentiality of *Connext* application.
- Potential crash of *Connext* application.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 5.8 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

Mitigations

- Protect access to the file system from which *Connext* applications are loading identity certificate files.
- Set the `com.rti.serv.secure.files_poll_interval` property value to `0` and, when you want to change the identity certificate, programmatically call `DomainParticipant::set_qos()` in your application code.

CWE Classification

- `CWE-416`

CAPEC Classification

- `CAPEC-165`

Associated Issue IDs

- [CVE Issue ID CVE-2025-8410]
- [RTI Issue ID SEC-2781]

Affected RTI Connext Professional Releases

- Affected: 7.5.0 before 7.6.0

CVE-2025-6965

[Critical] Potential out-of-bounds write in RTI Recording Service during its initialization

An out-of-bounds write in *RTI Recording Service* could have occurred while initializing the application.

User Impact without Security

A vulnerability in *RTI Recording Service* while initializing could have resulted in the following:

- Out-of-bounds write while executing a malicious SQLite statement.
- Not remotely exploitable.

- Potential impact on the integrity and confidentiality of *RTI Recording Service*.
- Potential crash in *RTI Recording Service*.
- CVSS v3.1 Base Score: 5.8 Medium
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L
- CVSS v4.0 Base Score: 5.8 Medium
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Keep your local file system protected.

CWE Classification

- `CWE-197`

CAPEC Classification

- `CAPEC-100`

Associated Issue IDs

- [CVE Issue ID CVE-2025-6965]
- [RTI Issue ID RECORD-1541]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.0.10
- Affected: 6.1.0 before 6.1.2.27
- Affected: 6.0.0 before 6.0.1.43

CVE-2025-4993

[Critical] Potential invalid read memory access in Connext applications during endpoint discovery

An invalid read memory access in *Connext* applications could have occurred while discovering a *DataWriter* or *DataReader*.

User Impact without Security

A vulnerability in *Connext* applications while discovering a *DataWriter* or *DataReader* could have resulted in the following:

- Out-of-bounds read while parsing a malicious RTPS message.
- Remotely exploitable.
- Potential impact on the confidentiality of *Connext* applications.
- Potential crash in the application.
- CVSS v3.1 Base Score: 9.1 Critical
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 8.3 High
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

There is no impact when enabling certain Security features; see Mitigations for more information.

Mitigations

Use *Security Plugins* RTPS protection, discovery protection, or RTPS PSK protection.

CWE Classification

- `CWE-822`

CAPEC Classification

- `CAPEC-129`

Associated Issue IDs

- [CVE Issue ID CVE-2025-4993]
- [RTI Issue ID CORE-15789]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.0.10
- Affected: 6.1.0 before 6.1.2.27
- Affected: 6.0.0 before 6.0.1.43
- Affected: 5.3.0 before 5.3.*
- Affected: 4.4a before 5.2.*

CVE-2025-1255

[Critical] Potential invalid read memory access in Connext applications when subscribing to PublicationBuiltinTopicData

An invalid read memory access in *Connext* applications could have occurred after calling `DDS_Subscriber_lookup_datareader` to retrieve the builtin publication information and then discovering a *DataWriter*.

User Impact without Security

A vulnerability in *Connext* applications while discovering a *DataWriter* could have resulted in the following:

- Out-of-bounds read while parsing a malicious RTPS message.
- Remotely exploitable.
- Potential impact on the confidentiality of *Connext* applications.
- Potential crash in the application.
- CVSS v3.1 Base Score: 9.1 Critical
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- CVSS v4.0 Base Score: 8.3 High
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N

User Impact with Security

There is no impact when enabling certain Security features; see Mitigations for more information.

Mitigations

- Use *Security Plugins* RTPS protection, discovery protection, or RTPS PSK protection.
- Set verbosity to `NDDS_CONFIG_LOG_VERBOSITY_WARNING` or higher for the `NDDS_CONFIG_LOG_CATEGORY_API` category.

CWE Classification

- `CWE-822`

CAPEC Classification

- `CAPEC-129`

Associated Issue IDs

- [CVE Issue ID CVE-2025-1255]
- [RTI Issue ID CORE-15730]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.2.0 before 7.3.0.9

Acknowledgments

Found by Ryan Shih <ryan.p.shih.civ@army.mil>

CVE-2025-4582

[Critical] Potential heap buffer read overflow in Connext applications when using a malicious license string

An out-of-bounds read on the heap could occur while parsing a malicious license string property (e.g., `dds.license.license_string`) value.

User Impact without Security

A vulnerability in the *Connext* application could have resulted in the following:

- Heap buffer overread while parsing a malicious license string.
- Exploitable by overwriting the XML QoS document on the file system with a malicious XML QoS document.
- Potential impact on confidentiality of *Connext* application.
- CVSS v3.1 Base Score: 4.4 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L
- CVSS v4.0 Base Score: 4.8 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Protect access to the file system from which *Connext* applications are loading XML QoS documents.
- Programmatically add the `dds.license.license_string` in your application code.
- Instead of using `dds.license.license_string`, use any of the other license methods described in https://community.rti.com/static/documentation/connext-dds/current/doc/manuals/connext_dds_professional/installation_guide/installation_guide/Li

cense_Management.htm#3.1_Installing_the_License_File. For example, put a file called **rti_license.dat** in your current working directory.

CWE Classification

- `CWE-126`, `CWE-193`

CAPEC Classification

- `CAPEC-165`, `CAPEC-540`

Associated Issue IDs

- [CVE Issue ID CVE-2025-4582]
- [RTI Issue ID CORE-15693]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.0.8
- Affected: 6.1.0 before 6.1.2.26
- Affected: 6.0.0 before 6.0.1.43
- Affected: 5.3.0 before 5.3.*
- Affected: 4.4a before 5.2.*

CVE-2024-12798

[Critical] Potential code injection in Admin Console when parsing malicious configuration file

Admin Console depended on logback-core 1.4.11, which is known to be affected by CVE-2024-12798 and CVE-2024-12801 publicly disclosed vulnerabilities.

This vulnerability has been fixed by upgrading logback-core to the latest stable version, 1.5.18.

User Impact without Security

This vulnerability could have resulted in the following:

- Exploitable by compromising the logback configuration file in the *Admin Console* installation, or by injecting an environment variable before executing *Admin Console*.
- CVSS v3.1 Score: 6.1 MEDIUM.
- CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:L
- CVSS v4.0 Score: 5.9 MEDIUM.
- CVSS v4.0 Vector: AV:L/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect the directory where Connext is installed from modifications by unauthorized users.

CWE Classification

- `CWE-917`

CAPEC Classification

- `CAPEC-242`

Associated Issue IDs

- [CVE Issue ID CVE-2024-12798, CVE-2024-12801]
- [RTI Issue ID ADMINCONSOLE-1432]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.*
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 5.2.0 before 5.2.*

CVE-2024-12801

[Critical] Potential code injection in Admin Console when parsing malicious configuration file

Admin Console depended on logback-core 1.4.11, which is known to be affected by CVE-2024-12798 and CVE-2024-12801 publicly disclosed vulnerabilities.

This vulnerability has been fixed by upgrading logback-core to the latest stable version, 1.5.18.

User Impact without Security

This vulnerability could have resulted in the following:

- Exploitable by compromising the logback configuration file in the *Admin Console* installation, or by injecting an environment variable before executing *Admin Console*.

- CVSS v3.1 Score: 6.1 MEDIUM.
- CVSS v3.1 Vector: AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:L
- CVSS v4.0 Score: 5.9 MEDIUM.
- CVSS v4.0 Vector: AV:L/AC:L/AT:P/PR:L/UI:P/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect the directory where Connext is installed from modifications by unauthorized users.

CWE Classification

- `CWE-917`

CAPEC Classification

- `CAPEC-242`

Associated Issue IDs

- [CVE Issue ID CVE-2024-12798, CVE-2024-12801]
- [RTI Issue ID ADMINCONSOLE-1432]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.6.0
- Affected: 7.0.0 before 7.3.*
- Affected: 6.1.0 before 6.1.*
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 5.2.0 before 5.2.*

RTI-SB-2025-05

Products and versions affected

- *RTI® Connext®* Professional Versions affected: 4.x to 7.5.0

Newly identified vulnerabilities

RTI has recently identified several new vulnerabilities, and a fix is available to address all the vulnerabilities. Type of issues:

- CWE-120: Buffer Copy without Checking Size of Input
- CWE-121: Stack-Based Buffer Overflow
- CWE-122: Heap-Based Buffer Overflow
- CWE-125: Out-of-Bounds Read
- CWE-190: Integer Overflow or Wraparound
- CWE-787: Out-of-Bounds Write

This is a detailed list of the issues included in this Security Bulletin, in spreadsheet format, for your convenience.

Available patches and best practices

A patch for long-term support versions of *Connext* is available on the RTI Customer Portal:

- *Connext Professional* 7.3.0.7 for 7.3.0
- *Connext Professional* 6.1.2.23 for 6.1.2

Please contact support@rti.com to arrange for a patch on other versions and architectures, or if you do not see the patch listed in the portal.

In addition to the patches mentioned above, all the fixes in this Security Bulletin are included in the latest *Connext Professional* 7.5.0.

VEX document snapshots for this Security Bulletin

If your *Connext* version is different than these, then use the general VEX documents above, which include our latest assessment of third-party-related vulnerabilities.

Product	VEX File
Connext Professional 7.3.0.7	Download
Connext Professional 6.1.2.23	Download

CVE-2025-1254

[Critical] Potential out-of-bounds read and write in Recording Service while using file rollover

Recording Service may have read or written out-of-bounds and crashed when recording using the rollover feature.

User Impact without Security

- Memory corruption leading to data corruption or a crash.
- Exploitable only when a race condition was won.
- Potential impact on confidentiality of the *Connext* application.
- When rollover was set up to change files based on size, exploitable through a compromised local file system containing a malicious database file.
- When rollover was set up to change files based on size, exploitable by publishing data over the network.
- CVSS 4.0 Base Score: 7.7 HIGH
- CVSS 4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- CVSS 3.1 Base Score: 8.8 HIGH
- CVSS 3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

User Impact with Security

- Memory corruption leading to data corruption or a crash.
- Exploitable only when a race condition was won.
- Potential impact on confidentiality of the *Connext* application.
- When rollover was set up to change files based on size, exploitable through a compromised local file system containing a malicious database file.
- CVSS 4.0 Base Score: 7.3 HIGH
- CVSS 4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- CVSS 3.1 Base Score: 7.8 HIGH
- CVSS 3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Mitigations

Protect access to the local file system where Recording Service is going to store data.

Use Security for topics being accepted by Recording Service.

CWE Classification

- `CWE-125`, `CWE-787`

CAPEC Classification

- `CAPEC-100`, `CAPEC-540`

Associated Issue IDs

- [CVE Issue ID CVE-2025-1254]
- [RTI Issue ID RECORD-1514]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.7
- Affected: 6.1.0 before 6.1.2.23
- Affected: 6.0.0 before 6.0.1.42

CVE-2025-1253

[Critical] Potential stack buffer write overflow in license-managed Core Libraries when setting RTI_LICENSE_FILE environment variable

The stack may have been corrupted while loading the `RTI_LICENSE_FILE` environment variable.

User Impact without Security

This vulnerability could have caused the following on any application loading the license information through the `RTI_LICENSE_FILE` environment variable:

- Stack corruption leading to data corruption or crash.
- Exploitable through a compromised local file system containing a malicious license file referenced by the `RTI_LICENSE_FILE` environment variable.
- CVSS 3.1 Base Score: 7.1 HIGH
- CVSS 3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS 4.0 Base Score: 6.9 MEDIUM
- CVSS 4.0 Vector: AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which Connext applications are loading license files.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2025-1253]
- [RTI Issue ID CORE-15310]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.7
- Affected: 6.1.0 before 6.1.2.23
- Affected: 6.0.0 before 6.0.1.42
- Affected: 5.3.0 before 5.3.*
- Affected: 4.5c before 5.2.*

CVE-2025-1252

[Critical] Potential buffer write overflow in Connext applications while parsing malicious license file

An out-of-bounds write on the heap could occur while parsing a malicious license file.

User Impact without Security

A vulnerability in the *Connext* application could have resulted in the following:

- Heap buffer overflow while parsing a malicious license file.
- Exploitable by overwriting the license file on the file system with a malicious license file.
- Potential impact on integrity and availability of *Connext* application.
- CVSS 3.1 Base Score: 7.1 HIGH
- CVSS 3.1 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS 4.0 Base Score: 6.9 MEDIUM
- CVSS 4.0 Vector: AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Protect access to the file system from which *Connext* applications are loading license files.

CWE Classification

- `CWE-122`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2025-1252]
- [RTI Issue ID CORE-15145]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.7
- Affected: 6.1.0 before 6.1.2.23
- Affected: 6.0.0 before 6.0.1.42
- Affected: 5.3.0 before 5.3.*
- Affected: 4.4d before 5.2.*

CVE-2024-45491

[Critical] Potential integer overflow in Connext applications on 32-bit systems when parsing XML files with very large number of default attributes or levels of nesting

The Core Libraries XML parser had a third-party dependency on Expat version 2.6.2, which is known to be affected by a number of publicly disclosed vulnerabilities. These vulnerabilities have been fixed by upgrading Expat to the latest stable version, 2.6.3. See the “What’s New” section in this document for more details.

The impact on *Connext* applications of using the previous version varied depending on your *Connext* application configuration:

User Impact without Security

- Exploitable through a compromised local file system containing malicious XML/DTD files.
- Remotely exploitable through malicious RTPS messages.
- If exploited, impact ranged from denial of service to potentially arbitrary code execution.
- 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

User Impact with Security

- Exploitable through a compromised local file system containing malicious XML/DTD files.
- If exploited, impact ranged from denial of service to potentially arbitrary code execution.
- 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

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND

- Restrict permissions for writing to the configuration files your *Connext* application uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-190`

CAPEC Classification

- `CAPEC-92`

Associated Issue IDs

- [CVE Issue ID CVE-2024-45491, CVE-2024-45492]
- [RTI Issue ID CORE-15121]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.7
- Affected: 6.1.0 before 6.1.2.23
- Affected: 6.0.0 before 6.0.1.42
- Affected: 5.3.0 before 5.3.*
- Affected: 4.3x before 5.2.*

CVE-2024-45492

[Critical] Potential integer overflow in Connext applications on 32-bit systems when parsing XML files with very large number of default attributes or levels of nesting

The Core Libraries XML parser had a third-party dependency on Expat version 2.6.2, which is known to be affected by a number of publicly disclosed vulnerabilities. These vulnerabilities have been fixed by upgrading Expat to the latest stable version, 2.6.3. See the “What’s New” section in this document for more details.

The impact on *Connext* applications of using the previous version varied depending on your *Connext* application configuration:

User Impact without Security

- Exploitable through a compromised local file system containing malicious XML/DTD files.
- Remotely exploitable through malicious RTPS messages.
- If exploited, impact ranged from denial of service to potentially arbitrary code execution.
- 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

User Impact with Security

- Exploitable through a compromised local file system containing malicious XML/DTD files.
- If exploited, impact ranged from denial of service to potentially arbitrary code execution.
- 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

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files your *Connext* application uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-190`

CAPEC Classification

- `CAPEC-92`

Associated Issue IDs

- [CVE Issue ID CVE-2024-45491, CVE-2024-45492]
- [RTI Issue ID CORE-15121]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.7
- Affected: 6.1.0 before 6.1.2.23
- Affected: 6.0.0 before 6.0.1.42
- Affected: 5.3.0 before 5.3.*
- Affected: 4.3x before 5.2.*

Previous Security Advisories

In the following we present a list of previous Security Advisories related to Connext products.

2024

CVE-2024-52066

[Critical] Potential stack corruption in Routing Service when using a malicious XML configuration document

An out-of-bounds write on the stack in *Routing Service* could have occurred after loading a malicious XML QoS document.

User Impact without Security

A vulnerability in *Routing Service* while loading configurations via XML could have resulted in the following:

- *Routing Service* could corrupt the stack.
- Exploitable by providing a malicious XML document to *Routing Service* during startup or via remote administration.
- Potential impact on the integrity of *Routing Service* when using the XML QoS document.
- Potential crash in the application.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Routing Service* while loading configurations via XML could have resulted in the following:

- *Routing Service* could corrupt the stack.
- Exploitable by providing a malicious XML document to *Routing Service* during startup.
- Potential impact on the integrity of *Routing Service* when using the XML QoS document.
- Potential crash in the application.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector (or a Governance Document with a value other than `NONE` for a `*_protection_kind` that applies to the *Routing Service's* remote administration topics), AND

- Restrict permissions for writing to the configuration files *Routing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52066]
- [RTI Issue ID ROUTING-1257]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40

CVE-2024-52065

[Critical] Potential stack buffer write overflow in Persistence Service while parsing malicious environment variable on non-Windows systems

An out-of-bounds write on the stack could occur while parsing a malicious environment variable on non-Windows systems.

User Impact without Security

A vulnerability in the *Persistence Service* application could have resulted in the following:

- Stack buffer overflow while parsing a malicious environment variable on non-Windows systems.
- Exploitable by overwriting the `.environment` file in the user's home directory with a malicious `.environment` file.
- Potential impact on integrity of Persistence Service application.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Protect access to the file system from which *Persistence Service* is running.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52065]
- [RTI Issue ID PERSISTENCE-362]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.2
- Affected: 6.1.1.2 before 6.1.2.21
- Affected: 5.3.1.40 before 5.3.1.41

CVE-2024-52064

[Critical] Potential stack buffer write overflow in Connext applications while parsing malicious license file

An out-of-bounds write on the stack could occur while parsing a malicious license file.

User Impact without Security

A vulnerability in the *Connext* application could have resulted in the following:

- Stack buffer overflow while parsing a malicious license file.
- Exploitable by overwriting the license file on the file system with a malicious license file.
- Potential impact on integrity of *Connext* application.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Protect access to the file system from which *Connext* applications are loading license files.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52064]
- [RTI Issue ID CORE-14875]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.2
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 4.4x before 5.2.*

CVE-2024-52063

[Critical] Potential stack buffer write overflow in Connext applications while parsing malicious XML types document

An out-of-bounds write on the stack could have occurred while parsing a malicious XML types document.

User Impact without Security

A vulnerability in the Core Libraries affected all products that load types via XML, and could have resulted in the following:

- Stack buffer overflow while parsing a malicious XML types document.
- Exploitable by changing an XML configuration file on the file system.
- Potential impact on the integrity of the application(s) using the XML types document.
- Potential crash in the application.

- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in "User Impact without Security" above.

Mitigations

- Restrict permissions for writing to *Connext* XML type files, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52063]
- [RTI Issue ID CORE-14872]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 4.4x before 5.2.*

[Critical] Potential stack buffer write overflow in Routing Service when parsing malicious XML types document

An out-of-bounds write on the stack in *Routing Service* could have occurred while parsing a malicious XML types document.

User Impact without Security

A vulnerability in *Routing Service* loading types via XML could have resulted in the following:

- Stack buffer overflow while parsing a malicious XML types document.

- Exploitable by changing an XML configuration file on the file system.
- Potential impact on the integrity of *Routing Service*.
- Potential crash in *Routing Service*.
- In *Routing Service*, the vulnerability could potentially be triggered through the remote administration command `load`.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Routing Service* loading types via XML could have resulted in the following:

- Stack buffer overflow while parsing a malicious XML types document.
- Exploitable by changing an XML configuration file on the file system.
- Potential impact on the integrity of *Routing Service*.
- Potential crash in *Routing Service*.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Routing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52063]
- [RTI Issue ID ROUTING-1238]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 4.4x before 5.2.*

CVE-2024-52062

[Critical] Potential stack buffer write overflow in Connext applications while parsing malicious XML types document

An out-of-bounds write on the stack could have occurred while parsing a malicious XML types document.

User Impact without Security

A vulnerability in the Core Libraries affected all products that load types via XML, and could have resulted in the following:

- Stack buffer overflow while parsing a malicious XML types document.
- Exploitable by changing an XML configuration file on the file system.
- Potential impact on the integrity of the application(s) using the XML types document. Such applications could include *Routing Service*.
- Potential crash in the application.
- In the case of *Routing Service*, the vulnerability could potentially have been triggered through the remote administration command load, but a successful attack would have required a malicious XML include file to already exist in the system, so the “Attack Vector” score is still “Local”.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Restrict permissions for writing to the *Connext* XML configuration files, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52062]
- [RTI Issue ID CORE-14871]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 4.4x before 5.2.*

CVE-2024-52061

[Critical] Potential stack buffer overflow in Connext applications when parsing an XML type

The stack may have been corrupted when parsing an XML type.

User Impact without Security

This vulnerability could have caused the following on any application using XML types:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through malicious RTPS messages.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could have caused the following on any application using XML types:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through a compromised local file system containing a malicious XML file.

- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Restrict permissions for writing to *Connext* XML type files, to prevent the Local Attack Vector, AND
- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector. Alternatively, enable *Security Plugins* endpoint discovery protection by setting `discovery_protection_kind` to a value other than NONE and setting `enable_discovery_protection` to TRUE in your Governance Document.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52061]
- [RTI Issue ID CORE-14870]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 5.0.0 before 5.2.*

[Critical] Potential stack buffer overflow in Routing Service when discovering types or loading XML types with certain characteristics

The stack could have been corrupted when *Routing Service* discovered a malicious type or loaded a malicious XML type.

User Impact without Security

This vulnerability could cause the following in *Routing Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through malicious RTPS messages.
- Exploitable through a compromised local file system containing a malicious XML file.
- *Routing Service* could be exploited by using a remote `load` administration command with a malicious XML type.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could cause the following in *Routing Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Restrict permissions for writing to the configuration files *Routing Service* uses, to prevent the Local Attack Vector, AND
- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52061]
- [RTI Issue ID ROUTING-1235]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 5.0.0 before 5.2.*

[Critical] Potential stack buffer overflow in Queuing Service when discovering type or loading XML type with certain characteristics

The stack could have been corrupted when *Queuing Service* discovered a malicious type or loaded a malicious XML type.

User Impact without Security

This vulnerability could cause the following in *Queuing Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through malicious RTPS messages.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could cause the following in *Queuing Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Restrict permissions for writing to the configuration files *Queueing Service* uses, to prevent the Local Attack Vector, AND

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector. Alternatively, enable *Security Plugins* endpoint discovery protection by setting `discovery_protection_kind` to a value other than NONE and setting `enable_discovery_protection` to TRUE in your Governance Document.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52061]
- [RTI Issue ID QUEUEING-791]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 5.0.0 before 5.2.*

[Critical] Potential stack buffer overflow in Recording Service when discovering type or loading XML type with certain characteristics

The stack could have been corrupted when *Recording Service* discovered a malicious type or loaded a malicious XML type.

User Impact without Security

This vulnerability could cause the following in *Recording Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through malicious RTPS messages.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 8.3 HIGH

- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

This vulnerability could cause the following in *Recording Service*:

- Stack corruption leading to data corruption or crash.
- Unbounded memory growth.
- Exploitable through a compromised local file system containing a malicious XML file.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

- Restrict permissions for writing to the configuration files *Recording Service* uses, to prevent the Local Attack Vector, AND
- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector. Alternatively, enable *Security Plugins* endpoint discovery protection by setting `discovery_protection_kind` to a value other than NONE and setting `enable_discovery_protection` to TRUE in your Governance Document.

CWE Classification

- `CWE-120`, `CWE-121`, `CWE-193`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52061]
- [RTI Issue ID RECORD-1508]

Affected RTI Connext Professional Releases

- Affected: 7.4.0 before 7.5.0
- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45
- Affected: 5.0.0 before 5.2.*

CVE-2024-52060

[Critical] Potential stack overflow in Cloud Discovery Service when using XML configuration file referencing environment variables

An out-of-bounds write on the stack in *Cloud Discovery Service* could have occurred while parsing XML files containing references to external environment variables.

User Impact without Security

This problem could have resulted in the following:

- Stack buffer overflow in *Cloud Discovery Service* when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Restrict permissions for writing to the configuration files *Cloud Discovery Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52060]
- [RTI Issue ID CDS-256]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21

- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45

[Critical] Potential stack overflow in Collector Service when using XML configuration file referencing environment variables

An out-of-bounds write on the stack in *Collector Service* could have occurred while parsing XML files containing references to external environment variables.

User Impact without Security

This vulnerability in *Observability Collector Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Restrict permissions for writing to the configuration files *Observability Collector Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52060]
- [RTI Issue ID OCA-360]

Affected RTI Connext Professional Releases

- Affected: 7.1.0 before 7.3.0.5

[Critical] Potential stack overflow in Queuing Service when using XML configuration file referencing environment variables

An out-of-bounds write on the stack in *Queuing Service* could occur while parsing XML files containing references to external environment variables.

User Impact without Security

This problem could result in the following:

- Stack buffer overflow in *Queuing Service* when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Restrict permissions for writing to the configuration files *Queuing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52060]
- [RTI Issue ID QUEUEING-784]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45

[Critical] Potential stack overflow in Recording Service when using XML configuration file referencing environment variables

An out-of-bounds write on the stack in *Recording Service* could have occurred while parsing XML files containing references to external environment variables.

User Impact without Security

A vulnerability in *Recording Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Restrict permissions for writing to the configuration files *Recording Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52060]
- [RTI Issue ID RECORD-1486]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40

[Critical] Potential stack overflow in Routing Service when using XML configuration file referencing environment variables

An out-of-bounds write on the stack in *Routing Service* could have occurred while parsing XML files containing references to external environment variables.

User Impact without Security

A vulnerability in *Routing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- Routing Service could be exploited by using a remote `load` administration command with malicious XML code.
- CVSS v3.1 Base Score: 8.2 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 8.3 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

User Impact with Security

A vulnerability in *Routing Service* could have resulted in the following:

- Stack buffer overflow when parsing a malicious XML file.
- Exploitable by providing malicious XML code to the applications during startup.
- A Governance Document that has a value other than NONE for a *_protection_kind that applies to the Routing Service's remote administration topics would defend against any attacks over the network.
- CVSS v3.1 Base Score: 6.1 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Routing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-120`, `CWE-121`

CAPEC Classification

- `CAPEC-10`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52060]
- [RTI Issue ID ROUTING-1223]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.5
- Affected: 6.1.0 before 6.1.2.21
- Affected: 6.0.0 before 6.0.1.40
- Affected: 5.3.0 before 5.3.1.45

CVE-2024-52059

[Critical] Potential heap buffer overflow in Security Plugins while creating a DomainParticipant that uses a malformed Identity Certificate

The *Security Plugins* were affected by a heap buffer overflow vulnerability that occurred while creating a *DomainParticipant* that used a malformed Identity Certificate.

User Impact without Security

Not applicable to this product.

User Impact with Security

The impact on *Security Plugins* applications of using the previous version was as follows:

- Exploitable by overwriting the Identity Certificate on the file system with a malicious Identity Certificate that does not even need to be properly signed by the Identity CA.
- The application could have experienced a heap buffer overwrite during creation of a new *DomainParticipant* that attempted to use the malicious Identity Certificate, impacting the integrity and availability of the application.
- This problem was much easier to exploit on a 32-bit architecture. On a 64-bit architecture, this problem affected only the Security Plugins for OpenSSL, not wolfSSL.
- The problem was only exploitable if the `authentication.propagate_simplified_identity_certificate` property was unset or set to `TRUE`.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- CVSS v4.0 Base Score: 6.9 MEDIUM
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N

Mitigations

Any one of the following steps is sufficient to mitigate the problem:

- Protect access to the file system from which *Connext* applications are loading certificates.
- Use the `data:,` prefix to specify the `dds.sec.auth.identity_certificate` property value.
- Set the `authentication.propagate_simplified_identity_certificate` property to `FALSE`.
- If available for your platform, use wolfSSL instead of OpenSSL. This mitigation only works if your architecture is 64-bit.

CWE Classification

- `CWE-120`, `CWE-122`, `CWE-190`

CAPEC Classification

- `CAPEC-46`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52059]
- [RTI Issue ID SEC-2444]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.2
- Affected: 6.1.0 before 6.1.2.17

CVE-2024-52058

[Major] Potential arbitrary command execution in System Designer while parsing malicious HTTP/REST requests

There was the potential for arbitrary command execution while parsing malicious HTTP/REST requests.

User Impact without Security

An improper neutralization of special elements used in *System Designer* HTTP/REST requests could have resulted in the following:

- Arbitrary command execution.
- Remotely exploitable from the same host on which *System Designer* was running.
- CVSS v3.1 Base Score: 8.4 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS v4.0 Base Score: 8.6 HIGH

- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

User Impact with Security

Same impact as described in "User Impact without Security" above.

Mitigations

Limit privileges of the *System Designer* process and limit access to the host *System Designer* is running into.

CWE Classification

- `CWE-78`

CAPEC Classification

- `CAPEC-88`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52058]
- [RTI Issue ID SYSD-1218]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0.2
- Affected: 6.1.0 before 6.1.2.19

CVE-2024-52057

[Critical] Potential arbitrary SQL query execution in Queuing Service while parsing malicious remote commands or configuration files

There was the potential for arbitrary SQL query execution in *Queuing Service* while parsing malicious remote administration commands or loading a malicious configuration file. This vulnerability is now fixed.

User Impact without Security

A SQL Injection vulnerability in *Queuing Service* could have resulted in the following:

- Arbitrary SQL query execution.
- Remotely exploitable.
- Potential impact on integrity and confidentiality of *Queuing Service*.

- CVSS v3.1 Base Score: 9.1 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
- CVSS v4.0 Base Score: 9.1 CRITICAL
- CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

User Impact with Security

When enabling RTPS protection, the impact of the SQL Injection vulnerability in *Queuing Service* was reduced, resulting in the following:

- Arbitrary SQL query execution.
- Exploitable from the same host *Queuing Service* is running.
- Potential impact on integrity and confidentiality of *Queuing Service*.
- CVSS v3.1 Base Score: 7.1 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
- CVSS v4.0 Base Score: 8.4 HIGH
- CVSS v4.0 Vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Queuing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-89`

CAPEC Classification

- `CAPEC-66`

Associated Issue IDs

- [CVE Issue ID CVE-2024-52057]
- [RTI Issue ID QUEUEING-756]

Affected RTI Connext Professional Releases

- Affected: 7.0.0 before 7.3.0
- Affected: 6.1.0 before 6.1.2.17
- Affected: 6.0.0 before 6.0.*
- Affected: 5.3.0 before 5.3.*
- Affected: 5.2.0 before 5.2.*

CVE-2024-25724

[Critical] Potential buffer overflow in Cloud Discovery Service while parsing XML document

There was potential for a buffer overflow in *Cloud Discovery Service* while parsing an XML document.

User Impact without Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_CDS_Service_new` public API containing malicious parameters.
- Remotely exploitable through malicious RTPS messages.
- *Cloud Discovery Service* could crash or leak sensitive information. An attacker could compromise *Cloud Discovery Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 9.4 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

User Impact with Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_CDS_Service_new` public API containing malicious parameters.
- *Cloud Discovery Service* could crash or leak sensitive information. An attacker could compromise *Cloud Discovery Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 7.3 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Cloud Discovery Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2024-25724]

- [RTI Issue ID CDS-222]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.1
- Affected: 6.0.0 before 6.0.1.35
- Affected: 5.3.0 before 5.3.1.44

[Critical] Potential buffer overflow in Queuing Service while parsing an XML document.

Potential buffer overflow in *Queuing Service* while parsing an XML document.

User Impact without Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_QueuingService_new` public API containing malicious parameters.
- Remotely exploitable through malicious RTPS messages.
- *Queuing Service* could crash or leak sensitive information. An attacker could compromise *Queuing Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 9.4 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

User Impact with Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_QueuingService_new` public API containing malicious parameters.
- *Queuing Service* could crash or leak sensitive information. An attacker could compromise *Queuing Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 7.3 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Queuing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2024-25724]
- [RTI Issue ID QUEUEING-759]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.1
- Affected: 6.0.0 before 6.0.1.35
- Affected: 5.3.0 before 5.3.1.44

[Critical] Potential buffer overflow in Recording Service while parsing an XML document.

Potential buffer overflow in *Recording Service* while parsing an XML document.

User Impact without Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to `rti::recording::Service()` public API containing malicious parameters.
- Remotely exploitable through malicious RTPS messages.
- *Recording Service* could crash or leak sensitive information. An attacker could compromise *Recording Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 9.4 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

User Impact with Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `rti::recording::Service()` public API constructor containing malicious parameters.
- *Recording Service* could crash or leak sensitive information. An attacker could compromise *Recording Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 7.3 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Recording Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2024-25724]
- [RTI Issue ID RECORD-1418]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.1
- Affected: 6.0.0 before 6.0.1.35
- Affected: 5.3.0 before 5.3.1.44

[Critical] Potential buffer overflow in Routing Service while parsing an XML document.

Potential buffer overflow in *Routing Service* while parsing an XML document.

User Impact without Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_RoutingService_new` public API containing malicious parameters.
- Remotely exploitable through malicious RTPS messages.
- *Routing Service* could crash or leak sensitive information. An attacker could compromise *Routing Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 9.4 CRITICAL
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

User Impact with Security

- Exploitable through a compromised local file system containing a malicious XML file.
- Exploitable through a compromised call to the `RTI_RoutingService_new` public API containing malicious parameters.
- *Routing Service* could crash or leak sensitive information. An attacker could compromise *Routing Service* integrity or execute malicious code with system privileges.
- CVSS v3.1 Base Score: 7.3 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

Mitigations

- Use *Security Plugins* RTPS protection to prevent the Network Attack Vector, AND
- Restrict permissions for writing to the configuration files *Routing Service* uses, to prevent the Local Attack Vector.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2024-25724]
- [RTI Issue ID ROUTING-1092]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.1
- Affected: 6.0.0 before 6.0.1.35
- Affected: 5.3.0 before 5.3.1.44

Acknowledgments

Found by Philip Pettersson <ppettersson@zoox.com>

2023

CVE-2023-46219

[Critical] Potential deletion of HSTS data in Observability Collector Service when saving to an excessively long file name

Observability Collector Service had a third-party dependency on Curl 8.1.2, which is known to be affected by a number of publicly disclosed vulnerabilities. These vulnerabilities have been fixed by upgrading Curl to the latest stable version, 8.5.0.

User Impact without Security

This vulnerability affected *Connext* 7.2.0 applications using the *Observability Collector Service*, as follows:

- When saving HSTS data to an excessively long file name, Curl could end up removing all contents.
- Subsequent requests using that file were unaware of the HSTS status they should otherwise use.
- CVSS v3.1 Base Score: 5.3 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Ensure that name of the file where HSTS data will be saved isn’t close to the length limit imposed by the machine’s file system, or avoid using HSTS.

CWE Classification

- `CWE-641`

Associated Issue IDs

- [CVE Issue ID CVE-2023-46219]
- [RTI Issue ID OCA-324]

Affected RTI Connext Professional Releases

- Affected: 7.2.0 before 7.3.0

CVE-2023-38039

[Critical] Potential out-of-memory error in Observability Collector Service while parsing an endless series of headers

Observability Collector Service had a third-party dependency on Curl 8.1.2, which is known to be affected by a number of publicly disclosed vulnerabilities. These vulnerabilities have been fixed by upgrading Curl to the latest stable version, 8.5.0.

User Impact without Security

This vulnerability affected *Connext* 7.2.0 applications using *Observability Collector Service*, as follows:

- Exploitable by streaming an endless series of headers to the application using Curl.
- The application could run out of memory.
- CVSS v3.1 Base Score: 7.5 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

Configure *Observability Collector Service* to send its data to trust-worthy servers.

CWE Classification

- `CWE-770`

Associated Issue IDs

- [CVE Issue ID CVE-2023-38039]

- [RTI Issue ID OCA-303]

Affected RTI Connext Professional Releases

- Affected: 7.2.0 before 7.3.0

2021

CVE-2021-38487

[Critical] Potential network amplification and information exposure when receiving malicious data(p)

Potential network amplification and information exposure when receiving malicious data(p).

This issue was originally filed as an issue in the OMG DDS RTPS specification (DDSIRTP26-6), where a modified RTPS participant announcement packet can trigger unwanted traffic, and potentially be used as part of a DoS attack. The OMG later refiled this issue as an OMG DDS Security specification issue under DDSSEC12-94. DDSSEC12-94 has been resolved in the most recent version of the OMG DDS Security 1.2 specification.

User Impact without Security

- Not applicable. This attack is outside the threat model for DDS systems not using *Security Extensions*.

User Impact with Security

- Remotely exploitable.
- Target nodes are forced to generate additional discovery traffic, potentially flooding the network.
- Target nodes may leak sensitive information propagated through participant and endpoint discovery.
- CVSS 4.0 Base Score: 8.8 HIGH
- CVSS 4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N
- CVSS v3.1 Base Score: 8.2 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Mitigations

- For RTI Connext Professional 7.3.0 and later, enabling the *Security Plugins* RTPS PSK Protection with `dds.sec.access.rtps_psk_protection_kind=SIGN` fully mitigates both the amplification and information exposure attacks described above. To protect against

participant discovery information disclosure by network insiders who can capture traffic exchanged between participants, it is recommended to set `dds.sec.access.rtps_psk_protection_kind=ENCRYPT`.

- For RTI Connext Professional 6.1.0 through 7.3.0, enabling Participant Discovery Protection also fully mitigates both the amplification and information exposure attacks. However, version 6.1.0 does not provide mechanisms to protect against participant discovery information disclosure by network insiders capable of capturing participant traffic. To ensure stronger protection against these types of threats, upgrading to RTI Connext Professional 7.3.0 or later is recommended.

Associated Issue IDs

- [CVE Issue ID CVE-2021-38487]
- [RTI Issue IDs SEC-1446, SEC-1244]

Affected RTI Connext Professional Releases

- Affected: 4.1x before 6.1.0

CVE-2021-38435

[Critical] Potential crash upon receiving a corrupted data(p)

Potential crash upon receiving a corrupted data(p).

User Impact without Security

- Remotely exploitable.
- Application crash. Potentially affecting confidentiality/integrity of *Connext* application.
- CVSS v3.1 Base Score: 7.6 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

User Impact with Security

Same impact as described in “User Impact without Security” above.

Mitigations

- Protect access to the network *Connext* applications are running in.

CWE Classification

- `CWE-125`

Associated Issue IDs

- [CVE Issue ID CVE-2021-38435]
- [RTI Issue ID CORE-11751]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.0.3
- Affected: 6.0.0 before 6.0.1.25
- Affected: 5.3.0 before 5.3.1.35
- Affected: 4.1x before 4.5d.rev41

CVE-2021-38433

[Critical] Potential stack buffer overflow while parsing an XML document

Potential stack buffer overflow while parsing an XML document.

User Impact without Security

- Remotely exploitable.
- Application crash, remote code execution with *Connext* application privileges.
- CVSS v3.1 Base Score: 7.6 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

User Impact with Security

- Only exploitable from the same host where the *Connext* application is running.
- CVSS v3.1 Base Score: 6.6 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

Mitigations

- Protect access to the network *Connext* applications are running in, or use *Security Plugins* RTPS protection.
- Restrict permissions for writing to the configuration files your *Connext* application uses.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2021-38433]
- [RTI Issue ID CORE-11750]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.0.3
- Affected: 6.0.0 before 6.0.1.25
- Affected: 5.3.0 before 5.3.1.35
- Affected: 4.5x before 4.5d.rev41

CVE-2021-38427

[Critical] Potential stack buffer overflow while parsing an XML document

Potential stack buffer overflow while parsing an XML document.

User Impact without Security

- Remotely exploitable.
- Application crash, remote code execution with *Connext* application privileges.
- CVSS v3.1 Base Score: 7.6 HIGH
- CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

User Impact with Security

- Only exploitable from the same host where the *Connext* application is running.
- CVSS v3.1 Base Score: 6.6 MEDIUM
- CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

Mitigations

- Protect access to the network *Connext* applications are running in, or use *Security Plugins* RTPS protection.
- Restrict permissions for writing to the configuration files your *Connext* application uses.

CWE Classification

- `CWE-121`

Associated Issue IDs

- [CVE Issue ID CVE-2021-38427]
- [RTI Issue ID CORE-11749]

Affected RTI Connext Professional Releases

- Affected: 6.1.0 before 6.1.0.3
- Affected: 6.0.0 before 6.0.1.25
- Affected: 5.3.0 before 5.3.1.35
- Affected: 4.5x before 4.5d.rev41