

## Introduction

This page contains a list of all *RTI*® *Connexx*® vulnerabilities that have been published through the [CVE® Program](#).

### 📌 Note

Since this document only contains vulnerabilities published through the [CVE® Program](#), the vulnerabilities listed in this document are a subset of the vulnerabilities published in the RTI Security Notices.

To receive further updates on vulnerabilities found in RTI products, including those that are not disclosed through the public CVE, please subscribe to our security notification list by sending an email to [security@rti.com](mailto:security@rti.com).

If you believe you have found a vulnerability affecting RTI products, please report it to us by sending an email to [security@rti.com](mailto: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 *Connexx* installation directory) details the third-party software included in RTI's products. Starting in *Connexx* 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 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 [Connexx 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 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. To join or be removed from the RTI Security Notification list, please send a request with your contact and company/program information to [security@rti.com](mailto:security@rti.com).

## Security Advisories

Release versions affected by the vulnerabilities are indicated using the following nomenclature:

"Affected: [FIRST IMPACTED VERSION] before [FIRST NOT IMPACTED VERSION]". For example, "Affected: 7.0.0 before 7.3.0.5" means the vulnerability affects all *Connex*t 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 *Connex*t 7.x version series starting with 7.4.0.

## 2025

### 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 *Connex*t 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 *Connex* 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 Connex 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.\*

# 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 Connexxt 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 Connexxt 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.\*
- Affected: 5.3.0 before 5.3.\*
- Affected: 4.5c before 5.2.\*

## CVE-2025-1252

### **[Critical] Potential buffer write overflow in Connex 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 *Connex* 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 *Connex* application.
- CVSS Base Score: 7.1 HIGH
- CVSS v3.1 Vector: [AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H](#)

#### **User Impact with Security**

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

#### **Mitigations**

Protect access to the file system from which *Connex* 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 Connex 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.\*
- Affected: 5.3.0 before 5.3.\*
- Affected: 4.4x before 5.2.\*

# 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 *Connex*t 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 *Connex*t 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 *Connex*t 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 Connex 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 Connex 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 *Connex* 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 Connex 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 *Connex* 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 Connex 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 *Queueing 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 Connex 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 Observability Collector Service when using XML configuration file referencing environment variables**

An out-of-bounds write on the stack in *Observability 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 Connex 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 Connex 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 Connex 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 Connex 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.

## 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 *Connex*t 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 Connex 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-2024-45492

## **[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.\*
- Affected: 5.3.0 before 5.3.\*
- Affected: 4.3x before 5.2.\*

# CVE-2024-45491

## **[Critical]** Potential integer overflow in Connex 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 *Connex* applications of using the previous version varied depending on your *Connex* 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 *Connex* 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 Connex 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.\*
- Affected: 5.3.0 before 5.3.\*
- Affected: 4.3x 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 Connex 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\_QueueingService\_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\_QueueingService\_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 Connex 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 Connex 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](mailto: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 Connex Professional Releases

- Affected: 7.2.0 before 7.3.0

# 2021

## CVE-2021-38487

### **[Critical] Potential network amplification attack when receiving malicious data(p)**

Potential network amplification attack when receiving malicious data(p).

This issue was originally filed as an issue in the OMG DDS RTPS specification ([DDSI RTP26-6](#)), 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 OMG DDS Security 1.2 specification.

## User Impact without Security

- Not applicable. This attack is out of 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.
- 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:L/I:N/A:H](#)

## Mitigations

- Enable *Security Plugins* RTPS PSK Protection (7.3.0) or Participant Discovery Protection (6.1.0).

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

#### CWE Classification

- [CWE-121](#)

#### Associated Issue IDs

- [ CVE Issue ID [CVE-2021-38433](#) ]
- [ RTI Issue ID CORE-11750 ]

## Affected RTI Connex 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 *Connex*t 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 *Connex*t 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 *Connex*t applications are running in, or use *Security Plugins* RTPS protection.
- Restrict permissions for writing to the configuration files your *Connex*t application uses.

#### CWE Classification

- [CWE-121](#)

#### Associated Issue IDs

- [ CVE Issue ID [CVE-2021-38427](#) ]
- [ RTI Issue ID CORE-11749 ]

#### Affected RTI Connex 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