Buffer Over-read, Off-by-one Error vulnerability in RTI Connext Professional (Core Libraries) allows File Manipulation, Overread Buffers.

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-4582
State	PUBLISHED
Assigner	RTI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-23 18:15:32 UTC
Updated	2026-04-01 02:16:01 UTC
Description	Buffer Over-read, Off-by-one Error vulnerability in RTI Connext Professional (Core Libraries) allows File Manipulation, Over

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from 3f572a00-62e2-4423-959a-7ea25eff1638

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-126 | CWE-193 | CWE-126 CWE-126 Buffer Over-read | CWE-193 CWE-193 Off-by-one Error

Version	Source	Type	Score	Severity	Vector
4.0	3f572a00-62e2-4423-959a-7ea25eff1638	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rti	Connext Professional	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RTI	Connext Professional	affected 7.4.0 7.6.0 custom	Not specified
CNA	RTI	Connext Professional	affected 7.0.0 7.3.0.8 custom	Not specified
CNA	RTI	Connext Professional	affected 6.1.0 6.1.2.26 custom	Not specified
CNA	RTI	Connext Professional	affected 6.0.0 6.0.1.43 custom	Not specified
CNA	RTI	Connext Professional	affected 5.3.0 5.3.* custom	Not specified
CNA	RTI	Connext Professional	affected 4.4a 5.2.* custom	Not specified

References

Reference	Source	Link	Tags
www.rti.com/vulnerabilities	3f572a00-62e2-4423-959a-7ea25eff1638	www.rti.com	Mitigation, Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.