Buffer Over-read vulnerability in RTI Connext Professional (Core Libraries) allows Overread Buffers.

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-2394
State	PUBLISHED
Assigner	RTI
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 01:16:40 UTC
Updated	2026-04-01 14:23:37 UTC
Description	Buffer Over-read vulnerability in RTI Connext Professional (Core Libraries) allows Overread Buffers.This issue affects Conr

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from 3f572a00-62e2-4423-959a-7ea25eff1638

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/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

EPSS: 0.000320000 probability, percentile 0.093000000 (date 2026-04-01)

Problem Types: CWE-126 | CWE-126 CWE-126 Buffer Over-read

Version	Source	Type	Score	Severity	Vector
4.0	3f572a00-62e2-4423-959a-7ea25eff1638	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/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

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	RTI	Connext Professional	affected 7.4.0 7.7.0 custom	Not specified
CNA	RTI	Connext Professional	affected 7.0.0 7.3.1.1 custom	Not specified
CNA	RTI	Connext Professional	affected 6.1.0 6.1.* custom	Not specified
CNA	RTI	Connext Professional	affected 6.0.0 6.0.* custom	Not specified
CNA	RTI	Connext Professional	affected 5.3.0 5.3.* custom	Not specified
CNA	RTI	Connext Professional	affected 4.3x 5.2.* custom	Not specified

References

Reference	Source	Link	Tags
www.rti.com/vulnerabilities	3f572a00-62e2-4423-959a-7ea25eff1638	www.rti.com	
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report