INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 17:20 UTC

CVE-2026-2467: Critical Heap-Based Buffer Overflow in RTI Connext Professional Core Libraries

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0327
Type	CVE Vulnerability
CVE ID	CVE-2026-2467
Severity	CRITICAL
CVSS Base Score	9.8
Affected Products	RTI Connext Professional Core Libraries (specific versions unconfirmed, source: gemini/secondary)
Published	2026-06-17
Discovery Source	Gemini

Executive Summary

CVE-2026-2467 is reported as a critical heap-based buffer overflow in RTI Connext Professional Core Libraries, a middleware platform used extensively in real-time, safety-critical, and industrial control system environments. An unauthenticated remote attacker can send specially crafted network messages to trigger arbitrary code execution at the privilege level of the Connext process. Organizations running RTI Connext Professional in operational technology, defense, aerospace, or industrial automation environments should treat this as a priority remediation item pending official vendor confirmation.

Technical Analysis

CVE-2026-2467 describes a heap-based buffer overflow (CWE-122) in RTI Connext Professional Core Libraries, a commercial Data Distribution Service (DDS) middleware platform. The reported CVSS base score is 9.8, indicating network-accessible, low-complexity, no-privilege, no-user-interaction exploitation characteristics. An unauthenticated remote attacker can exploit the vulnerability by sending specially crafted DDS protocol messages, potentially achieving arbitrary code execution at the privilege level of the Connext Professional process. MITRE ATT&CK techniques T1059 (Command and Scripting Interpreter) and T1190 (Exploit Public-Facing Application) apply. Affected versions are unconfirmed at this time. IMPORTANT CONFIDENCE CAVEAT: NVD detail for CVE-2026-2467 was not confirmed in the provided source data. The listed NVD source entry references CVE-2026-46817, indicating a possible source mismatch in the research pipeline. All technical

specifics, including affected versions, patch identifiers, and CVSS vector, must be verified against official RTI (Wind River) security advisories and NVD before operational action.

Action Checklist

1. Step 1: Containment, Immediately identify all systems running RTI Connext Professional Core Libraries in your environment using your asset inventory (CIS 1.1). Apply network segmentation to isolate DDS-enabled hosts from untrusted networks; block inbound DDS protocol traffic (default UDP ports 7400-7413 and vendor-specific ranges) at perimeter and internal firewalls (NIST AC-4). Prioritize internet-facing and OT/ICS-adjacent deployments first.
2. Step 2: Detection, Query endpoint and network logs for anomalous inbound DDS traffic patterns targeting RTI Connext processes; look for unexpected process spawning or privilege escalation events originating from Connext service accounts (NIST AU-6, CIS 8.2). Monitor for network connections to unknown external IPs from hosts running Connext Professional. No confirmed IOC hashes or IP indicators are available from the current source data, monitor behavioral patterns only until official IOCs are published.
3. Step 3: Eradication, Obtain the official RTI (Wind River) security advisory for CVE-2026-2467 once vendor confirmation is available (via RTI security alerts or NVD update). Do not apply patches until verified against official RTI/Wind River advisory documentation. After patching, rotate credentials for any service accounts associated with Connext Professional processes (NIST AC-2, D3-CRO).
4. Step 4: Recovery, After patching, verify Connext process integrity by reviewing system initialization configuration and service account permissions (D3-SICA, NIST AC-6). Re-enable network connectivity incrementally, starting with isolated test environments. Confirm audit logging is active and capturing DDS process events post-remediation (NIST AU-2, AU-12). Validate that network segmentation controls remain in place.
5. Step 5: Post-Incident, Document control gaps exposed by this vulnerability: DDS middleware asset visibility, network segmentation coverage of OT/ICS-adjacent systems, and vulnerability management process coverage of industrial middleware (NIST IR-1, CIS 7.1, CIS 7.2). Review whether RTI Connext deployments appear in your software inventory (CIS 2.1) and whether patch management processes reach this product tier (CIS 7.3, CIS 7.4). Establish a vendor advisory monitoring process for RTI/Wind River products.

Detection Guidance

No confirmed IOC indicators (hashes, IPs, domains) are available from current source data. Detection should focus on behavioral indicators. Monitor for: (1) unexpected inbound connections to DDS protocol ports (UDP 7400-7413 and vendor-configured ranges) from external or untrusted network segments; (2) anomalous child process creation originating from RTI Connext Professional service processes; (3) memory fault events, crash dumps, or application restarts on hosts running Connext Professional; (4) privilege escalation events associated with the Connext process account. Relevant controls: NIST AU-6 (Audit Record Review), AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs). Apply D3-LAM (Local Account Monitoring) to Connext service accounts. All detection signatures should be developed against confirmed vendor-published technical details once the official RTI advisory is available.

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
CVE-2026-2467 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-2467	T3
CVE-2026-46817 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-46817	T1
CVE-2026-2467 | Tenable®	https://www.tenable.com/cve/CVE-2026-2467	T3

Source	URL	Tier
May 2026 CVE Landscape - Recorded Future	https://www.recordedfuture.com/blog/may-2026-cve-landscape	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-2467	T1

Generated 2026-06-18 17:20 UTC by TJS Security Command Center