INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 06:38 UTC

CVE-2026-43870: Apache Thrift Node.js web_server.js Multi-Vulnerability in Microsoft CBL-Mariner 2.0

CVE VULNERABILITY | CRITICAL | CVSS 9.4

SCC Item ID	SCC-CVE-2026-0138
Type	CVE Vulnerability
CVE ID	CVE-2026-43870
Severity	CRITICAL
CVSS Base Score	9.4
EPSS Score	0.0001 (0th percentile)
Affected Products	Microsoft CBL-Mariner 2.0, cbl2 ceph 16.2.10-11 (Apache Thrift Node.js web_server.js component)
Published	2026-05-07T01:12:35
Discovery Source	Msrc Patch Tuesday

Executive Summary

CVE-2026-43870 is a critical vulnerability (CVSS 9.4) in the Apache Thrift Node.js web_server.js component as shipped in Microsoft CBL-Mariner 2.0, disclosed during Microsoft Patch Tuesday May 2026. Organizations running CBL-Mariner 2.0 with the ceph 16.2.10-11 package are exposed to potential remote attack via a network-accessible RPC interface. No active exploitation has been confirmed, but the critical severity warrants prompt patching, as exploitation tooling historically emerges within 1-4 weeks of public disclosure for CVEs of this rating.

Technical Analysis

CVE-2026-43870 affects the Apache Thrift Node.js web_server.js component as packaged in Microsoft CBL-Mariner 2.0 (cbl2 ceph 16.2.10-11). CVSS base score: 9.4 (Critical). The 'multi-vulnerability' designation indicates multiple distinct weaknesses within the same component. Specific vulnerability classes have not been detailed in publicly available advisories as of this writing. Apache Thrift is an RPC framework; its Node.js server component exposes a network-accessible attack surface, mapping to MITRE ATT&CK T1190 (Exploit Public-Facing Application). No CWE IDs have been published. EPSS score is 0.006% (0.3rd percentile), indicating minimal current exploitation probability despite the critical CVSS rating. CVE is not listed on the CISA KEV catalog. Primary advisory: MSRC Update Guide

(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-43870). NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2026-43870. Verify all URLs are current before distribution; human validation is recommended. Patch details should be confirmed against the May 2026 MSRC CVRF feed at https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May if available.

Action Checklist

1. Step 1: Containment, Identify all CBL-Mariner 2.0 hosts running ceph 16.2.10-11 in your environment. If the Thrift web_server.js service is internet-facing, restrict access via firewall or security group rules to trusted source IPs until patching is complete. Check the MSRC Update Guide at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-43870 for any available mitigating configuration guidance.
2. Step 2: Detection, Query your asset inventory and CMDB for CBL-Mariner 2.0 nodes with ceph installed. On Linux hosts, run 'rpm -q ceph' or 'dnf list installed ceph' to confirm affected version 16.2.10-11. Review network flow logs for unexpected inbound connections to Thrift RPC ports (default 9090/TCP; verify against your deployment config). Check application logs in /var/log/ceph/ for anomalous request patterns or error spikes near the disclosure date.
3. Step 3: Eradication, Apply the updated ceph package for CBL-Mariner 2.0 as released by Microsoft. Monitor the MSRC Update Guide and CBL-Mariner package repository (https://packages.microsoft.com/cbl-mariner/) for the patched ceph version. CBL-Mariner 2.0 uses the tdnf (Tiny DNF) package manager; once the patched ceph version is available, run 'tdnf update ceph' on affected hosts. Confirm the patched package version resolves CVE-2026-43870 before deploying to production.
4. Step 4: Recovery, After patching, re-run 'rpm -q ceph' to verify the patched version is installed. Confirm the Thrift web_server.js service restarts cleanly and passes functional health checks. Re-enable any network access rules that were restricted during containment. Monitor application and network logs for 48-72 hours post-patch for any anomalous activity suggesting prior compromise.
5. Step 5: Lessons Learned & Control Improvements, Audit your CBL-Mariner 2.0 patch cadence: this CVE was disclosed via Patch Tuesday May 2026, so assess whether your patching SLA for critical-severity vulnerabilities was met. Evaluate whether Thrift RPC services require internet-facing exposure or can be restricted to internal network segments as a permanent control. Add CVE-2026-43870 to your next vulnerability review cycle and document remediation timelines for audit evidence.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and initiate formal incident declaration if: (1) network flow analysis reveals inbound connections to 9090/TCP from external IPs in the window between CVE-2026-43870 disclosure (Patch Tuesday May 2026) and containment firewall application, (2) /var/log/ceph/ shows deserialization exceptions or unexpected RPC errors coinciding with external connection timestamps indicating active exploitation, or (3) ceph-mgr processes exhibit unexpected child process spawning (indicative of RCE), at which point regulatory breach notification timelines must be assessed if the Ceph cluster hosts PII, PHI, or regulated data.

Recovery Notes	After applying the Microsoft-released patched ceph package via 'tdnf update ceph' on all CBL-Mariner 2.0 hosts, verify Ceph cluster health returns to HEALTH_OK status via 'ceph status' before re-enabling any externally-facing network access rules that were restricted during containment. Monitor /var/log/ceph/ceph-mgr.*.log and network flow data for inbound 9090/TCP sessions for a minimum of 72 hours post-patch — continued anomalous RPC traffic or ceph-mgr errors after patching should be treated as evidence of prior compromise requiring full forensic investigation. Confirm the sha256 hash of the deployed web_server.js matches the vendor-published value for the patched package before closing the incident.
Forensic Artifacts	/var/log/ceph/ceph-mgr.*.log — Primary artifact: deserialization exceptions, unexpected RPC parsing errors, or stack traces referencing web_server.js indicate exploitation attempts against CVE-2026-43870's Apache Thrift Node.js component. | Network flow records for 9090/TCP (or configured Thrift RPC port) — Source IP, byte count, connection duration, and frequency from external addresses in the 30-day window before and after Patch Tuesday May 2026 disclose whether reconnaissance or exploitation predated your awareness. | sha256 hash of /path/to/web_server.js (pre-patch) — Documents the vulnerable artifact state for chain-of-custody and confirms the specific vulnerable file version present; compare against the patched package's file hash to verify remediation. | Output of 'ps auxf | grep -E (ceph-mgr|node|thrift)' captured at time of containment — Reveals whether any unexpected child processes (shells, interpreters, reverse-connect tools) were spawned by the ceph-mgr process, which would indicate successful RCE via CVE-2026-43870. | Pre-containment 'ss -tnp state established sport = :9090 or dport = :9090' output — Documents active Thrift RPC sessions at the moment of isolation; any sessions from non-trusted IPs with unusual duration or byte ratios warrant deep-packet inspection of captured pcap evidence.

Per-Action IR Details

Step 1: Containment — Identify all CBL-Mariner 2.0 hosts running ceph 16.2.10-11 in your environment. If the Thrift web_server.js service is internet-facing, restrict access via firewall or security group rules to trusted source IPs until patching is complete. Check the MSRC Update Guide at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-43870 for any available mitigating configuration guidance.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent exploitation of the network-accessible Thrift RPC interface while preserving operational continuity.

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: On each CBL-Mariner 2.0 host, immediately apply a host-level firewall rule to block inbound 9090/TCP from non-trusted sources: 'sudo iptables -I INPUT -p tcp --dport 9090 ! -s -j DROP && sudo iptables-save > /etc/sysconfig/iptables'. Enumerate all exposed hosts with: 'for host in $(cat cbl-mariner-hosts.txt); do ssh $host "ss -tlnp | grep 9090"; done'. Cross-reference against your CMDB manually if automated discovery is unavailable.

Evidence: Before restricting firewall rules, capture a snapshot of current active connections to the Thrift RPC port: 'ss -tnp state established dport = :9090' and 'ss -tnp state established sport = :9090' — output reveals any sessions already in progress that may indicate pre-disclosure scanning or exploitation. Also capture 'netstat -an | grep 9090' and dump the current iptables ruleset with 'iptables -L -n -v' to document the pre-containment exposure window. Preserve these outputs as timestamped evidence per NIST AU-3 (Content of Audit Records).

Step 2: Detection — Query your asset inventory and CMDB for CBL-Mariner 2.0 nodes with ceph installed. On Linux hosts, run 'rpm -q ceph' or 'dnf list installed ceph' to confirm affected version 16.2.10-11. Review network flow logs for unexpected inbound connections to Thrift RPC ports (default 9090/TCP, verify against your deployment config). Check application logs in /var/log/ceph/ for anomalous request patterns or error

spikes near the disclosure date.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate package version telemetry, network flow anomalies on port 9090/TCP, and ceph application log error spikes to determine whether reconnaissance or exploitation attempts preceded the disclosure date.

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Use osquery to enumerate affected package versions across the fleet without a CMDB: 'osqueryi --json "SELECT name, version, source FROM deb_packages WHERE name LIKE \'ceph%\'" (or rpm_packages table on CBL-Mariner). For network detection without a SIEM, deploy a Sigma rule targeting port 9090 inbound connections in Zeek/Suricata logs: filter conn.log for 'id.resp_p=9090' with external source IPs. For log analysis, run: 'grep -E "(error|exception|traceback|WARN|unexpected)" /var/log/ceph/*.log | awk -F: \'{print $1}\' | sort | uniq -c | sort -rn' to surface error frequency spikes.

Evidence: Capture the full output of 'rpm -qa --queryformat "%{NAME} %{VERSION}-%{RELEASE}\n" | grep ceph' on each host to document the exact installed build. Preserve /var/log/ceph/ directory contents (ceph.log, ceph-mgr.*.log, ceph-mon.*.log) for the 30-day window preceding the May 2026 Patch Tuesday disclosure date — specifically hunting for malformed RPC request errors or unexpected deserialization exceptions in web_server.js that would indicate CVE-2026-43870 exploitation attempts via Apache Thrift's binary or compact protocol framing. Collect network flow records showing source IP, byte count, and connection duration for all inbound 9090/TCP sessions; anomalously short high-volume connections may indicate fuzzing or exploit delivery.

Step 3: Eradication — Apply the updated ceph package for CBL-Mariner 2.0 as released by Microsoft. Monitor the MSRC Update Guide and CBL-Mariner package repository (https://packages.microsoft.com/cbl-mariner/) for the patched ceph version. Use 'tdnf update ceph' on affected hosts once the fix is available. Confirm the patched package version resolves CVE-2026-43870 before deploying to production.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerable ceph 16.2.10-11 package containing the Apache Thrift web_server.js flaw from all CBL-Mariner 2.0 hosts and verify the patched build is confirmed by Microsoft as resolving CVE-2026-43870.

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST IR-4 (Incident Handling), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without an enterprise patch management platform, script the patch deployment: 'for host in $(cat affected-hosts.txt); do ssh $host "sudo tdnf update -y ceph && rpm -q ceph" | tee -a patch-log-$(date +%Y%m%d).txt; done'. Before patching production, validate the package signature: 'rpm --checksig .rpm' and confirm the GPG key matches Microsoft's CBL-Mariner signing key. Stage the patch on a non-production CBL-Mariner 2.0 node first and run 'ceph status' post-update to confirm the Ceph cluster does not degrade.

Evidence: Before executing 'tdnf update ceph', capture a pre-patch system state: 'rpm -qi ceph' (full package metadata including install date), 'sha256sum /usr/lib/node_modules/apache-thrift/lib/nodejs/lib/thrift/web_server.js' or equivalent path to the vulnerable web_server.js file — this hash documents the unpatched artifact for chain-of-custody. Also run 'ps aux | grep -E "(ceph|thrift|node)"' to capture all running Thrift/Node.js process instances that must be terminated as part of eradication. If prior exploitation is suspected, collect a memory dump of the ceph-mgr process before killing it.

Step 4: Recovery — After patching, re-run 'rpm -q ceph' to verify the patched version is installed. Confirm the Thrift web_server.js service restarts cleanly and passes functional health checks. Re-enable any network access rules that were restricted during containment. Monitor application and network logs for 48-72 hours post-patch for any anomalous activity suggesting prior compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore the ceph service to verified-clean operational state, confirm the patched web_server.js component loads correctly, and validate that the Thrift RPC interface responds only to authorized traffic before lifting containment firewall rules.

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Verify integrity of the patched web_server.js file: 'sha256sum /path/to/web_server.js' and compare against the vendor-published hash from the CBL-Mariner package manifest ('rpm -V ceph' will report any file-level deviations from the installed package). To monitor for post-patch anomalies without EDR, deploy a Sigma rule or manual cron job that alerts on new inbound 9090/TCP connections from external IPs: 'watch -n 60 "ss -tnp | grep :9090"'. Use Wireshark or tcpdump to capture a 10-minute sample of Thrift RPC traffic post-restart and inspect for malformed or unexpected protocol frames: 'tcpdump -i eth0 -w /tmp/thrift-postpatch.pcap port 9090'.

Evidence: Document the post-patch package state with 'rpm -qi ceph' and capture the output of 'ceph version' and 'ceph status' to confirm cluster health and the new daemon build strings. Preserve /var/log/ceph/ logs from the 48-72 hour post-patch monitoring window — any continued deserialization errors or unexpected RPC parsing failures in ceph-mgr logs during this period would indicate a threat actor established persistence prior to patching and is still active. Retain the pre- and post-patch sha256 hashes of web_server.js as integrity evidence per NIST SI-7 (Software, Firmware, and Information Integrity).

Step 5: Post-Incident — Audit your CBL-Mariner 2.0 patch cadence: this CVE was disclosed via Patch Tuesday May 2026, so assess whether your patching SLA for critical-severity vulnerabilities was met. Evaluate whether Thrift RPC services require internet-facing exposure or can be restricted to internal network segments as a permanent control. Add CVE-2026-43870 to your next vulnerability review cycle and document remediation timelines for audit evidence.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct a lessons-learned review measuring time-to-patch against your critical-severity SLA for CVE-2026-43870, assess whether permanent network segmentation of the Thrift RPC interface reduces future attack surface, and update detection content to catch exploitation attempts against Apache Thrift on CBL-Mariner.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Generate a remediation timeline report from your patch log files: 'grep -h "ceph" patch-log-*.txt | sort' to calculate mean time to remediate (MTTR) for CVE-2026-43870 against your critical-severity SLA. For the permanent segmentation control, codify the iptables rule restricting 9090/TCP into your CBL-Mariner 2.0 hardening baseline and enforce it via a startup script or systemd unit: 'ExecStartPost=/sbin/iptables -I INPUT -p tcp --dport 9090 ! -s -j DROP'. Publish a YARA rule targeting the vulnerable web_server.js file hash to detect any unpatched stragglers: 'rule CVE_2026_43870_unpatched_webserver { strings: $h = "" condition: $h }'.

Evidence: Compile audit evidence package: (1) timestamped output of 'rpm -q ceph' pre- and post-patch from all affected hosts, (2) firewall change logs showing the containment rule applied and the date/time of rule removal, (3) /var/log/ceph/ archives spanning disclosure date through patch completion, (4) the patch-log text file generated during eradication capturing per-host patch timestamps. This package satisfies NIST AU-11 (Audit Record Retention) requirements and supports demonstration of SLA compliance for critical CVEs if audited under a GRC framework.

Detection Guidance

On CBL-Mariner 2.0 hosts, confirm affected package presence with: 'rpm -qa | grep ceph', output showing ceph-16.2.10-11 confirms exposure. Check active Thrift service listeners with 'ss -tlnp | grep node' or 'netstat -tlnp | grep 9090' (adjust port per deployment). Review /var/log/ceph/ and Node.js application logs for

unexpected RPC request volumes, malformed request errors, or connection attempts from unexpected source IPs. In your SIEM, query for outbound connections from CBL-Mariner hosts to unusual external destinations, which could indicate post-exploitation callback activity. Map this activity to MITRE ATT&CK T1571 (Non-Standard Port) or T1008 (Fallback Channels) if command-and-control communication is suspected. The primary relevant technique is T1190 (Exploit Public-Facing Application); hunt for follow-on techniques T1059 (Command and Scripting Interpreter) or T1105 (Ingress Tool Transfer) on affected hosts if initial exploitation is suspected. No confirmed IOCs are available at this time.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-5** — Incident Monitoring

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

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-43870	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May	T1

Source	URL	Tier
CVE-2026-43870 | Tenable®	https://www.tenable.com/cve/CVE-2026-43870	T3
CVE-2026-43870 - CVE Details, Severity, and Analysis | Strobes VI	https://strobes.co/vi/cve/CVE-2026-43870/	T3
CVE-2026-43870 - Info Vulnerability - TheHackerWire	https://www.thehackerwire.com/vulnerability/CVE-2026-43870/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-43870	T1

Generated 2026-05-07 06:38 UTC by TJS Security Command Center