INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-07 19:05 UTC

CVE-2026-33109: Critical RCE in Azure Managed Instance for Apache Cassandra (CVSS 9.9)

CVE VULNERABILITY | CRITICAL | CVSS 9.9

SCC Item ID	SCC-CVE-2026-0139
Type	CVE Vulnerability
CVE ID	CVE-2026-33109
Severity	CRITICAL
CVSS Base Score	9.9
Affected Products	Microsoft Azure Managed Instance for Apache Cassandra
Published	2026-05-07T07:00:11
Discovery Source	Msrc Patch Tuesday

Executive Summary

Microsoft disclosed CVE-2026-33109, a critical remote code execution vulnerability in Azure Managed Instance for Apache Cassandra, as part of the May 2026 Patch Tuesday release. With a CVSS base score of 9.9, the flaw is network-accessible and likely exploitable without authentication at low complexity, meaning an attacker could execute arbitrary code on affected managed instances without requiring credentials. Organizations running this Azure service are exposed to full database compromise, data exfiltration, and potential lateral movement within their cloud environment until the Microsoft-issued patch is applied.

Technical Analysis

CVE-2026-33109 affects Microsoft Azure Managed Instance for Apache Cassandra. CVSS base score: 9.9 (critical). No CVSS vector string was included in available source data; the score implies network attack vector, low complexity, and no authentication required, though these components are inferred from the score and service architecture and have not been independently confirmed from the MSRC advisory at time of writing. No CWE classification was published with the disclosure; check NVD and MSRC for updated CWE mapping. No EPSS score or percentile is currently available (0.0 values reflect absent data, not zero probability). The vulnerability maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter), consistent with an unauthenticated RCE pathway leading to command execution on the managed node. CISA KEV listing: not present as of configuration date. Patch source: MSRC Update Guide for CVE-2026-33109 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33109). NVD entry:

https://nvd.nist.gov/vuln/detail/CVE-2026-33109. Note: EPSS data, confirmed CVSS vector, and exploit details were not available in the source material at the time of generation. Monitor MSRC and NVD for updates.

Action Checklist

1. Step 1: Containment, Identify all Azure Managed Instance for Apache Cassandra deployments in your subscription inventory. Restrict public endpoint access to known IP ranges via Azure Private Endpoints or network security group (NSG) rules immediately. Confirm whether the managed instance endpoint is exposed to the public internet and disable public access if not operationally required.
2. Step 2: Detection, Review Azure Monitor and Azure Diagnostic Logs for anomalous connection attempts, unexpected client IPs, and unusual query patterns against Cassandra managed instances. Check Azure Defender for Cloud (Microsoft Defender for Databases) alerts for any triggered detections referencing CVE-2026-33109 or suspicious remote execution activity. Query Azure Activity Logs for unauthorized management plane operations against the affected resource type.
3. Step 3: Eradication, Apply the patch issued by Microsoft via the MSRC Update Guide for CVE-2026-33109 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33109) when available. Verify patch release date and availability status in the MSRC advisory before assuming deployment readiness. For Azure managed services, confirm whether the patch is applied automatically by Microsoft or requires operator action; check the MSRC advisory for patch deployment model. If manual action is required, prioritize internet-exposed instances first.
4. Step 4: Recovery, After patch confirmation, validate that Azure Managed Instance for Apache Cassandra is running the patched version via the Azure portal or CLI. Re-enable any access that was restricted during containment only after patch status is confirmed. Monitor Defender for Cloud and Azure Monitor for 72 hours post-remediation for residual anomalous activity. Verify no unauthorized data was accessed by reviewing Cassandra audit logs and Azure Storage access logs for the instance.
5. Step 5: Post-Incident, Assess whether Azure Private Endpoint was already enforced for this service; if not, treat the gap as a control deficiency and remediate across all managed database services. Review your vulnerability management process for Azure PaaS services to ensure Patch Tuesday advisories trigger timely review of managed service offerings, not only IaaS. Update threat model documentation to reflect unauthenticated RCE as a realistic attack scenario for Azure managed database services.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/privacy counsel immediately if Azure Diagnostic Logs, Cassandra audit logs, or Azure Storage access logs show any evidence of unauthorized CQL queries, data reads, or outbound data transfers from the managed instance during the window between CVE-2026-33109 public disclosure and containment completion, as this constitutes a potential reportable data breach under GDPR Article 33, CCPA, or applicable state breach notification laws if the Cassandra instance holds PII, PHI, or financial data.

Recovery Notes	Do not lift NSG restrictions or re-enable public endpoints until `az managed-cassandra cluster show` confirms the patched Cassandra version matches the fixed version specified in the MSRC advisory for CVE-2026-33109, and until Cassandra audit logs have been reviewed for unauthorized data access during the exposure window. Monitor Microsoft Defender for Cloud alerts and Azure Monitor connection metrics for the Cassandra managed instance for a minimum of 72 hours post-patch, with particular attention to any new external IPs establishing CQL connections on TCP 9042 or 9142, which may indicate attacker re-entry attempts or scanning by threat actors aware of the CVE. If the instance was confirmed internet-exposed during the vulnerability window and audit logs are unavailable or show gaps, treat data confidentiality as unverifiable and initiate your breach notification assessment workflow.
Forensic Artifacts	Azure Network Watcher flow logs for TCP 9042 (Cassandra CQL) and TCP 9142 (Cassandra SSL CQL) on the subnet hosting the managed instance — these will show every source IP that reached the Cassandra endpoint and are the primary artifact for identifying attacker probe or exploit traffic targeting CVE-2026-33109. | Azure Diagnostic Logs for the Microsoft.DocumentDB/cassandraClusters resource type, specifically connection events and error logs — a successful or attempted unauthenticated RCE exploit against CVE-2026-33109 may produce anomalous error codes, JVM exceptions, or malformed protocol events in these logs that distinguish exploit attempts from legitimate client traffic. | Microsoft Defender for Cloud raw alert JSON for the Cassandra resource (`az security alert list`), which may contain pre-generated detections tagged to MITRE ATT&CK T1190 (Exploit Public-Facing Application) or T1059 (Command and Scripting Interpreter) if the RCE resulted in command execution observable at the platform monitoring layer. | Cassandra native audit log entries (if audit logging was enabled on the managed instance) showing CQL operation type, client IP, keyspace, and table accessed — SELECT or COPY operations against sensitive keyspaces from non-application IPs during the exposure window are the primary indicator of data exfiltration following a successful CVE-2026-33109 exploit. | Azure Activity Log entries for the Cassandra managed instance resource ID scoped to the 7 days preceding discovery — unauthorized management plane operations (PUT, DELETE, POST) from unexpected Azure AD principals or service principals may indicate an attacker used the RCE foothold to pivot to Azure control-plane access via instance metadata or managed identity credentials.

Per-Action IR Details

Step 1: Containment — Identify all Azure Managed Instance for Apache Cassandra deployments in your subscription inventory. Restrict public endpoint access to known IP ranges via Azure Private Endpoints or network security group (NSG) rules immediately. Confirm whether the managed instance endpoint is exposed to the public internet and disable public access if not operationally required.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected resources to prevent further exploitation of the unauthenticated RCE vector in CVE-2026-33109 while maintaining operational availability where possible.

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run `az resource list --resource-type Microsoft.DocumentDB/cassandraClusters --output table` to enumerate all Cassandra Managed Instance deployments across subscriptions. For each exposed instance, use `az network nsg rule create` to insert a DENY rule blocking inbound TCP 9042 (native Cassandra CQL port) and TCP 9142 (SSL CQL) from 0.0.0.0/0, allowing only your known application subnet CIDRs. If Private Endpoint is not yet configured, use `az network private-endpoint create` as an emergency measure. Document every change with timestamp and operator for the incident record.

Evidence: Before modifying NSG rules or enabling Private Endpoint, capture the current network exposure state: run `az network nsg rule list` for all NSGs associated with the Cassandra subnet and export to JSON. Pull Azure Network Watcher flow logs for TCP 9042 and TCP 9142 for the 72 hours preceding discovery to identify source IPs that reached the Cassandra endpoint — these are your candidate attacker IPs for IOC correlation. Export `az monitor activity-log list` filtered to the Cassandra resource for the same window to capture any management-plane changes made during the potential exploitation window.

Step 2: Detection — Review Azure Monitor and Azure Diagnostic Logs for anomalous connection attempts, unexpected client IPs, and unusual query patterns against Cassandra managed instances. Check Azure Defender for Cloud (Microsoft Defender for Databases) alerts for any triggered detections referencing CVE-2026-33109 or suspicious remote execution activity. Query Azure Activity Logs for unauthorized management plane operations against the affected resource type.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate multiple log sources to determine whether CVE-2026-33109 was exploited prior to containment, and establish the scope of any unauthorized code execution on the managed instance.

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use Azure CLI to query logs directly: `az monitor log-analytics query --workspace --analytics-query "AzureDiagnostics | where ResourceType == 'CASSANDRACLUSTERS' | where TimeGenerated > ago(7d) | where clientIPAddress_s !in () | summarize count() by clientIPAddress_s, bin(TimeGenerated, 1h)"`. For Defender for Cloud alerts without a SIEM integration, export the alerts via `az security alert list --resource-group --output json` and grep for severity 'High' or 'Critical'. For management plane abuse, run `az monitor activity-log list --resource-id --start-time --caller-filter` and look for PUT/DELETE/POST operations from unexpected principal IDs or service principals not associated with your automation accounts.

Evidence: Capture the following before analyst review modifies log retention state: (1) Azure Diagnostic Logs for the Cassandra managed instance showing all CQL connection events — specifically client IP, timestamp, and any error codes indicating malformed or oversized requests that may indicate exploit probe traffic against CVE-2026-33109. (2) Microsoft Defender for Cloud raw alert JSON for the resource, which may contain MITRE ATT&CK technique tags for T1190 (Exploit Public-Facing Application) if exploitation was detected. (3) Azure Monitor Metrics for the instance showing CPU spikes, memory anomalies, or unusual disk I/O at times correlated with unexpected external connection attempts — a successful RCE would likely cause a process execution spike visible in compute metrics.

Step 3: Eradication — Apply the patch issued by Microsoft via the MSRC Update Guide for CVE-2026-33109 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33109). For Azure managed services, confirm whether the patch is applied automatically by Microsoft or requires operator action; check the MSRC advisory for patch deployment model. If manual action is required, prioritize internet-exposed instances first.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability enabling unauthenticated RCE by confirming patch application to the Azure Managed Instance for Apache Cassandra service layer, and verify no backdoor or persistence mechanism was installed during any exploitation window.

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Confirm patch deployment model via the MSRC advisory page for CVE-2026-33109 — Azure PaaS services often auto-patch, but operator confirmation is required. Use `az managed-cassandra cluster show --resource-group --cluster-name --query 'properties.provisioningState'` to verify cluster state post-patch. If the advisory indicates a version string change, use `az managed-cassandra cluster show` to retrieve the `cassandraVersion` property and compare against the patched version listed in the MSRC advisory. If the instance was potentially compromised prior to patching, treat it as a suspect system: snapshot the OS disk of any associated data nodes before patching using `az snapshot create`, preserving forensic state. Do not rely solely on patch application — scan for web

shells or unexpected processes that may have been deployed via the RCE vector.

Evidence: Before applying the patch, preserve: (1) Current `az managed-cassandra cluster show` output in full JSON, capturing the pre-patch version string and configuration state as a baseline for post-patch comparison. (2) If Microsoft provides node-level access or diagnostic bundles for the managed instance, capture any Cassandra system logs (`/var/log/cassandra/system.log`) showing startup events, unusual JVM errors, or references to deserialization or reflection activity that may indicate exploit attempts against the RCE mechanism. (3) Azure Resource Graph snapshot: `az graph query -q "Resources | where type == 'microsoft.documentdb/cassandraclusters"'` to document the pre-patch resource configuration across all subscriptions.

Step 4: Recovery — After patch confirmation, validate that Azure Managed Instance for Apache Cassandra is running the patched version via the Azure portal or CLI. Re-enable any access that was restricted during containment only after patch status is confirmed. Monitor Defender for Cloud and Azure Monitor for 72 hours post-remediation for residual anomalous activity. Verify no unauthorized data was accessed by reviewing Cassandra audit logs and Azure Storage access logs for the instance.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore the Azure Managed Instance for Apache Cassandra to a known-good operational state, validate patch integrity, and confirm no attacker persistence or data exfiltration occurred before lifting containment controls.

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), NIST SI-6 (Security and Privacy Function Verification), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Validate patched version with `az managed-cassandra cluster show --resource-group --cluster-name --output json | jq '.properties.cassandraVersion'` and confirm against the MSRC advisory's fixed version. For Cassandra audit log review without a SIEM, enable Cassandra audit logging if not already active (verify via `az managed-cassandra cluster show` for audit configuration properties), then pull logs via Azure Diagnostic Log export to a storage account and parse with `az storage blob download` piped to `grep` for operations from unexpected principals or during the suspicious timeframe. For Azure Storage access logs tied to the instance's backup or data export destinations, use `az storage logging show` and review access logs for GET operations against Cassandra data blobs from IPs matching your candidate attacker list from Step 1 evidence.

Evidence: Before re-enabling public access or lifting NSG restrictions, capture: (1) Cassandra audit log entries (if audit logging was enabled) for the exploitation window — specifically CQL operations of type SELECT, INSERT, or USE from client IPs not in your known application inventory, which would indicate data access or reconnaissance by an attacker who achieved RCE. (2) Azure Storage access logs for any storage account associated with Cassandra backups, showing any unexpected read or copy operations that may indicate data exfiltration via the RCE foothold. (3) Azure Monitor 'Requests' metric for the Cassandra instance scoped to the 7 days preceding discovery, exported as CSV, to identify any sustained high-volume query activity from a single external IP consistent with bulk data extraction.

Step 5: Post-Incident — Assess whether Azure Private Endpoint was already enforced for this service; if not, treat the gap as a control deficiency and remediate across all managed database services. Review your vulnerability management process for Azure PaaS services to ensure Patch Tuesday advisories trigger timely review of managed service offerings, not only IaaS. Update threat model documentation to reflect unauthenticated RCE as a realistic attack scenario for Azure managed database services.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: use lessons learned from CVE-2026-33109 to drive systemic improvements to Azure PaaS visibility, network isolation standards, and Patch Tuesday review workflows for managed database services.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CM-2 (Baseline Configuration), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team without enterprise tooling: create an Azure Policy assignment using the built-in policy `Deny public network access for Azure Managed Instance for Apache Cassandra` (policy definition ID available via `az policy definition list --query "[?contains(displayName, 'Cassandra')]"`) to enforce Private Endpoint as a hard control going forward. For Patch Tuesday monitoring of PaaS services, subscribe to the MSRC Security Update Guide RSS feed filtered to the 'Azure' product family and set a calendar-blocked review within 24 hours of each second Tuesday. Use the free Microsoft Defender for Cloud regulatory compliance dashboard (no additional cost in Azure) to track Private Endpoint enforcement status across all managed database resource types.

Evidence: For the post-incident review record, compile: (1) Timeline delta between Microsoft's public disclosure of CVE-2026-33109 (May 2026 Patch Tuesday) and your organization's first containment action — this gap is a measurable process metric for the lessons-learned report. (2) Azure Policy compliance report showing which managed database services (Cassandra, Cosmos DB, Azure SQL Managed Instance, Azure Database for PostgreSQL) lacked Private Endpoint enforcement at the time of disclosure, establishing the true blast radius of the control gap. (3) The NSG and network flow log evidence captured in Step 1 and Step 2, retained per your audit record retention policy (NIST AU-11), as these constitute the incident evidentiary record and may be required for breach notification assessment if data access is confirmed.

Detection Guidance

No confirmed IOCs or active exploitation indicators were available in source data at time of writing. Detection should focus on behavioral indicators. In Azure Monitor, query for unusual inbound connections to your Cassandra managed instance endpoint, particularly from unexpected source IPs or geographies. In Microsoft Defender for Cloud, enable and review Defender for Databases coverage for the Cassandra managed instance (verify current product name in Microsoft Defender for Cloud documentation, as Defender product naming may have been updated after this item was generated). Review Azure NSG flow logs for connection attempts on Cassandra default ports (9042, 7000, 7001, 9160) from external or unexpected internal sources. Query Azure Activity Logs for CreateOrUpdate or Delete operations on the managed instance resource type from unfamiliar principals. If Azure Sentinel (Microsoft Sentinel) is deployed, create an analytic rule alerting on anomalous authentication failures or connection bursts against the managed instance. Monitor NVD and MSRC for published CVSS vector details and exploit proof-of-concept that may sharpen detection signatures.

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
- **A.5.23** — Information security for use of cloud services

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
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33109	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May	T1
(consolidated)	https://www.securityweek.com/critical-remote-code-execution-vulnera...	T3
Exploitation of 'Copy Fail' Linux Vulnerability Begins - SecurityWeek	https://www.securityweek.com/exploitation-of-copy-fail-linux-vulner...	T3
Warning Over Critical CopyFail Linux Kernel Vulnerability Now ...	https://www.secureblink.com/cyber-security-news/warning-over-critic...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-33109	T1

Generated 2026-05-07 19:05 UTC by TJS Security Command Center