INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-17 13:50 UTC

Azure Backup for AKS Confused Deputy Vulnerability Enabled Cluster-Admin Privilege Escalation, Silent Fix, No CVE Issued

SECURITY ANALYSIS | CRITICAL | CVSS 9.5

SCC Item ID	SCC-STY-2026-0140
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft Azure Backup for AKS, Azure Kubernetes Service (AKS)
Published	2026-05-16T16:55:44
Discovery Source	Rss

Executive Summary

A security researcher discovered that Azure Backup for AKS could be exploited to escalate a low-privilege Backup Contributor identity to full cluster-admin control over any targeted AKS cluster, without any direct Kubernetes permissions. Microsoft rejected the vulnerability report, blocked CVE assignment, and publicly denied changes, yet the attack path ceased to work and new permission validation logic appeared in the service, indicating a silent, unacknowledged fix. The incident signals a broader governance risk: when cloud vendors remediate silently and deny disclosure, security teams lose the audit trail needed to assess exposure windows, verify remediation, and meet compliance obligations.

Technical Analysis

The vulnerability is a textbook Confused Deputy attack (CWE-441) against Azure Backup for AKS. The Backup Contributor role is designed for backup operators, it carries no direct Kubernetes RBAC permissions. However, the Azure Backup service itself operates with elevated trust inside the AKS control plane. A researcher demonstrated that a user holding only the Backup Contributor role could invoke backup service APIs in a way that caused the service to act as an unintended proxy, exercising its own elevated context on behalf of the attacker. The result was a cluster-admin binding on the target cluster, full read/write/execute control over every workload, secret, namespace, and node in the cluster.

The attack chain maps clearly to the MITRE ATT&CK framework. The initial foothold requires only a Valid Cloud Account with the Backup Contributor role (T1078.004), a low bar in environments where backup permissions are distributed broadly or provisioned through IaC without role-minimization reviews. The Confused Deputy

mechanism itself constitutes Abuse of Elevation Control Mechanism (T1548) and Access Token Manipulation (T1134), as the attacker leverages the service's trusted identity rather than their own. Once cluster-admin is obtained, downstream actions could include deploying malicious containers (T1610), exfiltrating secrets and persistent volumes from cloud storage (T1530), or adding persistent backdoor accounts (T1098.003).

The CVSS base score of 9.5 reflects the attack's profile accurately: network-accessible, low complexity, no user interaction required, and high impact across confidentiality, integrity, and availability. The absence of a CVE, however, means this score exists only in the researcher's report, not in any vendor advisory, vulnerability database, or scanner feed that security teams rely on for prioritization.

Microsoft's response is the story's most consequential element for the security community. The company rejected the report through its standard disclosure channel, blocked CVE assignment, and issued a public denial of any changes. The silent remediation, confirmed by the attack path no longer functioning and observable changes to permission validation logic in the service, contradicts that denial. This is not a novel pattern: cloud vendors have historically applied silent fixes to avoid CVE-linked SLA obligations and public scrutiny. But in this case, the affected system is Kubernetes cluster infrastructure, where a successful exploit grants an attacker the equivalent of domain administrator access over containerized workloads.

Security teams now face a gap with no standard closure path. There is no CVE to track, no vendor advisory to reference, no patch version to verify, and no official remediation guidance. The exposure window, the period between when the vulnerability was exploitable and when the silent fix took effect, is unknown. Organizations cannot determine whether the Backup Contributor role was abused against their clusters during that window without building detection logic retroactively. AKS audit logs, Kubernetes API server logs, and Azure Activity Logs are the primary forensic surfaces, but without a known timeline from the vendor, log retention limits may already have consumed the relevant window.

The disclosure pattern also undermines the coordinated vulnerability disclosure model that the security community depends on. When vendors control CVE assignment through their own CNA authority and deny changes after silent remediation, researchers have no effective escalation path, and defenders receive no signal. CISA's Known Exploited Vulnerabilities catalog, scanner plugins, and SIEM detection rules are all downstream of CVE assignment, none of them fire when there is no CVE to fire on.

Action Checklist

1. Assess exposure: Determine whether your organization uses Azure Backup for AKS. Identify every AKS cluster with backup configured and enumerate all identities holding the Backup Contributor role, including service principals, managed identities, and human accounts.
2. Audit role assignments: Pull Azure RBAC role assignments for the Backup Contributor role across all subscriptions. Flag any identity that holds this role and is not a tightly controlled, dedicated backup service identity. Remove or downscope unnecessary assignments immediately.
3. Review Kubernetes audit logs: Query AKS audit logs for unexpected cluster-admin bindings, ClusterRoleBinding or RoleBinding creation events, and API calls originating from Azure Backup service identities that fall outside expected backup operation patterns. Focus the review on the widest available retention window.
4. Review Azure Activity Logs: Examine Activity Logs for anomalous invocations of Azure Backup for AKS APIs, particularly restore or configuration operations initiated by identities not associated with approved backup workflows.

5. Apply least-privilege to backup roles: Enforce strict scope limits on Backup Contributor assignments, restrict to the minimum required resource scope, audit quarterly, and require justification for any human identity holding this role.

6. Update threat model: Add Confused Deputy attacks against cloud-managed service roles as a threat scenario in your AKS and Azure threat register, mapped to T1548, T1078.004, and T1098.003.

7. Communicate findings to leadership: Brief leadership on the exposure with specific context: the affected product, the absence of a vendor advisory, the unknown exposure window, and the steps taken to audit and harden role assignments.

8. Monitor for follow-up disclosure: Track the original researcher's publications, security news outlets, and Microsoft Security Response Center (MSRC) advisories for any subsequent CVE assignment or official remediation guidance. Set a calendar reminder to re-evaluate in 30 days if no official advisory appears.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if the Kubernetes audit log review (step 3) reveals any ClusterRoleBinding creation event attributable to a Backup Contributor identity outside of expected backup operations — this indicates potential exploitation during the unknown exposure window and may trigger breach notification obligations if AKS workloads process PII, PHI, or PCI-scoped data.
Recovery Notes	After containment and role rescoping, verify that legitimate AKS backup operations continue to function correctly by confirming successful backup job completion via `az dataprotection job list --vault-name --resource-group --output table` — failed jobs post-remediation may indicate over-scoped role removal. Monitor AKS cluster-admin ClusterRoleBindings daily for 30 days using `kubectl get clusterrolebindings -o json | jq '.items[] | select(.roleRef.name=="cluster-admin")'` to detect any re-emergence of unauthorized bindings. Given that the exposure window is unknown and Microsoft has not issued a CVE or confirmed the attack path publicly, maintain heightened monitoring posture until an official MSRC advisory is published or Microsoft support confirms the fix status in writing.

Forensic Artifacts	Azure RBAC role assignment export (JSON) capturing all Backup Contributor principals with principalId, principalType, scope, createdOn, and createdBy — this documents the confused deputy attack surface as it existed and is required to reconstruct the potential exploitation pathway if post-incident analysis reveals compromise | Kubernetes kube-audit log entries for ClusterRoleBinding and RoleBinding create/patch/delete events — the exploit mechanism would manifest as an unexpected ClusterRoleBinding granting cluster-admin to an attacker-controlled identity, with the requestor being the Azure Backup trusted service identity rather than a human administrator | Azure Activity Log records for Microsoft.DataProtection/backupVaults/backupInstances/restore/action and /write operations, with caller identity, correlationId, clientIpAddress, and eventTimestamp — the correlationId links the Azure control-plane invocation to the downstream Kubernetes API server audit event, establishing the confused deputy chain | Kubernetes ClusterRoleBinding YAML snapshot (`kubectl get clusterrolebindings -o yaml`) capturing all current cluster-admin bindings with their subjects and creationTimestamps — any binding with a creationTimestamp during the exposure window and a non-human, Azure-service-linked subject is a high-confidence exploitation indicator | Azure Backup for AKS backup instance configuration export (`az dataprotection backup-instance list --output json`) capturing the trusted identity associated with each backup vault and cluster pairing — this establishes which specific managed identity held the trusted service role and is the entity whose actions must be traced across both the Azure Activity Log and Kubernetes audit log

Per-Action IR Details

Assess exposure: Determine whether your organization uses Azure Backup for AKS. Identify every AKS cluster with backup configured and enumerate all identities holding the Backup Contributor role, including service principals, managed identities, and human accounts.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: scope and impact assessment of the affected environment

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST RA-2 (Security Categorization), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run: `az role assignment list --role 'Backup Contributor' --all-namespaces --output table` across each subscription via Azure CLI to enumerate all principals. Cross-reference against a manually maintained spreadsheet of approved backup service identities. For managed identity enumeration: `az identity list --output table` and check each against backup vault configurations with `az dataprotection backup-vault list --output table`.

Evidence: Before scoping, preserve a point-in-time snapshot of current Azure RBAC role assignments: `az role assignment list --all --output json > rbac_snapshot_$(date +%Y%m%d).json`. Capture AKS cluster list with backup vault associations: `az aks list --output json` and `az dataprotection backup-instance list --vault-name --resource-group --output json`. These baselines establish what was in place before any remediation and are required if the unknown exposure window necessitates post-incident review.

Audit role assignments: Pull Azure RBAC role assignments for the Backup Contributor role across all subscriptions. Flag any identity that holds this role and is not a tightly controlled, dedicated backup service identity. Remove or downscope unnecessary assignments immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolating the privilege pathway exploited by the confused deputy attack

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Export full Backup Contributor assignments across all subscriptions: `az role assignment list --role 'Backup Contributor' --all --output json | jq '.[] | {principal: .principalName, type: .principalType, scope: .scope}'`. For immediate removal of any non-service-identity holder: `az role assignment delete --assignee --role 'Backup Contributor' --scope `. Maintain a change log with timestamps and approver names for audit defensibility. A 2-person team can divide subscriptions and run in parallel using the Azure CLI in separate terminal sessions.

Evidence: Preserve the pre-removal role assignment export (JSON with principalId, principalName, principalType, roleDefinitionName, scope, and createdOn fields) before executing any deletions — this documents the attack surface as it existed and is critical evidence if the exposure window analysis later reveals exploitation. Also capture: `az role assignment list --role 'Backup Contributor' --all --include-groups --output json > backup_contributor_pre_remediation.json`.

Review Kubernetes audit logs: Query AKS audit logs for unexpected cluster-admin bindings, ClusterRoleBinding or RoleBinding creation events, and API calls originating from Azure Backup service identities that fall outside expected backup operation patterns. Focus the review on the widest available retention window.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: evidence correlation to determine whether exploitation occurred during the unknown exposure window

Controls: NIST AU-2 (Event Logging), 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: Enable AKS audit logging to Log Analytics if not already active: Diagnostic Settings → kube-audit and kube-audit-admin log categories. Query Log Analytics (free tier supports limited retention): `AzureDiagnostics | where Category == 'kube-audit' | where log_s contains 'ClusterRoleBinding' or log_s contains 'RoleBinding' | where log_s contains 'cluster-admin' | project TimeGenerated, log_s`. For clusters without Log Analytics, download raw audit logs via: `az aks get-credentials` then use `kubectl get events --all-namespaces` and review existing ClusterRoleBindings: `kubectl get clusterrolebindings -o json | jq '.items[] | select(.roleRef.name=="cluster-admin") | {name: .metadata.name, subjects: .subjects, creationTimestamp: .metadata.creationTimestamp}'`.

Evidence: The confused deputy exploit would produce Kubernetes API server audit events showing: (1) ClusterRoleBinding creation events with `verb: create`, `resource: clusterrolebindings`, `requestURI` containing `/apis/rbac.authorization.k8s.io/v1/clusterrolebindings`, and a `user.username` or `user.groups` value corresponding to the Azure Backup managed identity or service principal; (2) subsequent API calls with cluster-admin privilege from that same identity performing actions beyond read/write on backup-related resources (PVCs, VolumeSnapshots). Capture: `kubectl get clusterrolebindings -o yaml > clusterrolebindings_snapshot.yaml` and export kube-audit logs covering the maximum available retention window before any cluster modification.

Review Azure Activity Logs: Examine Activity Logs for anomalous invocations of Azure Backup for AKS APIs, particularly restore or configuration operations initiated by identities not associated with approved backup workflows.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlating Azure control-plane activity with the confused deputy attack chain to determine if the privilege escalation pathway was invoked

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query Azure Activity Logs via CLI for Backup for AKS operations: `az monitor activity-log list --start-time 2024-01-01 --offset 90d --query "[?resourceProvider=='Microsoft.DataProtection' && (contains(operationName.value,'BackupInstance') || contains(operationName.value,'RestoreInstance'))]" --output json`. Filter for caller identities and cross-reference against approved backup service principal list. Export to JSON for offline analysis: append `> activity_log_backup_ops.json`. Focus specifically on `Microsoft.DataProtection/backupVaults/backupInstances/restore/action` and `Microsoft.DataProtection/backupVaults/backupInstances/write` operation names triggered by unexpected callers.

Evidence: The confused deputy attack requires invoking Azure Backup for AKS restore or configuration operations to cause the trusted Azure Backup service identity to act on behalf of the attacker. Activity Log entries to capture and preserve include: operationName (specifically restore/action and backupInstances/write), caller UPN or service principal objectId, correlationId (links Azure control-plane action to downstream Kubernetes API server actions), httpRequest.clientIpAddress, and eventTimestamp. Export the full 90-day Activity Log retention window: `az monitor activity-log list --max-events 10000 --output json > activity_log_full_export.json`.

Apply least-privilege to backup roles: Enforce strict scope limits on Backup Contributor assignments — restrict to the minimum required resource scope, audit quarterly, and require justification for any human identity holding this role.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: removing the structural conditions that made the confused deputy attack possible, specifically over-broad Backup Contributor scope

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Scope Backup Contributor assignments to the specific backup vault resource ID rather than subscription or resource group: `az role assignment create --assignee --role 'Backup Contributor' --scope /subscriptions//resourceGroups//providers/Microsoft.DataProtection/backupVaults/`. Script a quarterly audit job using Azure CLI scheduled via cron or Azure Automation: `az role assignment list --role 'Backup Contributor' --all --output json | jq '.[] | select(.scope | contains("subscriptions") and (contains("resourceGroups") | not))'` — this flags any subscription-scope assignments for immediate review. Document every human-held Backup Contributor assignment with ticket reference.

Evidence: Before rescoping assignments, capture the current scope configuration for each Backup Contributor assignment (principalId, principalType, scope path, createdOn, createdBy) as a signed, timestamped artifact. This documents the pre-remediation attack surface width and is required for the post-incident lessons-learned report. Also record the backup vault's `TrustedServiceList` and any cross-tenant delegation settings if present.

Update threat model: Add Confused Deputy attacks against cloud-managed service roles as a threat scenario in your AKS and Azure threat register, mapped to T1548, T1078.004, and T1098.003.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned and threat model improvement to prevent recurrence across analogous cloud managed service integrations

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SA-11 (Developer Testing and Evaluation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Add the following three MITRE ATT&CK technique entries to your Azure/AKS threat register with this-incident-specific notes: T1548 (Abuse Elevation Control Mechanism) — Azure Backup for AKS trusted service identity used as a confused deputy to elevate Backup Contributor to cluster-admin; T1078.004 (Valid Accounts: Cloud Accounts) — attacker leverages legitimately assigned Backup Contributor managed identity as the initial vector; T1098.003 (Account Manipulation: Add Office 365 Global Admin Role) — generalized to Kubernetes ClusterRoleBinding manipulation granting cluster-admin to attacker-controlled identity. Use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to layer these techniques and export the JSON layer for your threat register. Extend the model to cover analogous Azure managed services (Azure Defender for Containers, Azure Monitor, Azure Policy) that similarly receive elevated Kubernetes permissions.

Evidence: The threat model update should reference the specific evidence artifacts collected in steps 3 and 4: the ClusterRoleBinding snapshot, kube-audit log export, and Activity Log export. These constitute the empirical basis for the threat scenario entry and should be attached or linked in the threat register record to distinguish this entry from a hypothetical scenario.

Communicate findings to leadership: Brief leadership on the exposure with specific context: the affected product, the absence of a vendor advisory, the unknown exposure window, and the steps taken to audit and

harden role assignments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: organizational communication of incident findings, including disclosure to leadership with accurate characterization of residual risk

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST IR-4 (Incident Handling), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Structure the leadership brief around five specific data points: (1) product affected — Azure Backup for AKS, vendor-confirmed silently patched with no CVE issued; (2) blast radius — list the exact count of AKS clusters and Backup Contributor identities identified in step 1; (3) exposure window — unknown start date to approximate patch date; (4) evidence of exploitation — binary outcome from audit log review in steps 3 and 4; (5) remediation status — role scoping actions taken with timestamps. Use the NIST IR-6 reporting template structure as a framework for the brief. A 2-person team can produce this brief using the JSON exports from steps 1–4 as supporting data without additional tooling.

Evidence: Attach the following artifacts to the leadership brief package as supporting evidence: rbac_snapshot_pre_remediation.json (step 2), clusterrolebindings_snapshot.yaml (step 3), activity_log_backup_ops.json (step 4), and the role rescoping change log from step 5. These provide a complete, timestamped audit trail of the exposure and response. The absence of a CVE and the silent fix history should be explicitly noted as creating an unquantifiable residual risk — this is a material fact for leadership decision-making on whether to engage Microsoft support for incident verification.

Monitor for follow-up disclosure: Track the original researcher's publications, BleepingComputer coverage, and MSRC advisories for any subsequent CVE assignment or official remediation guidance. Set a calendar reminder to re-evaluate in 30 days if no official advisory appears.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: sustained monitoring for new intelligence that would change the incident's risk characterization or require additional response actions

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Configure free RSS or web monitoring for the following specific sources without a paid tool: (1) MSRC Security Update Guide filtered for 'Azure Backup' and 'AKS' — RSS feed available at https://api.msrc.microsoft.com/update-guide/rss; (2) the original researcher's blog or GitHub — set a Google Alert for their name combined with 'Azure Backup AKS'; (3) BleepingComputer — RSS feed for 'Microsoft' tag; (4) CISA Known Exploited Vulnerabilities catalog — `curl https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | jq '.vulnerabilities[] | select(.vendorProject=="Microsoft")' > kev_microsoft_check.json` run weekly via cron. Create a shared team calendar event for 30-day re-evaluation with the specific decision criteria: if no official advisory by then, escalate to formal vendor engagement via Microsoft support case.

Evidence: At the 30-day re-evaluation checkpoint, re-run the AKS ClusterRoleBinding audit (`kubectl get clusterrolebindings -o json | jq '.items[] | select(.roleRef.name=="cluster-admin")'`) and the Backup Contributor RBAC export to confirm no new unexpected assignments have appeared. This serves as both a monitoring artifact and evidence of ongoing due diligence in the absence of an official vendor advisory. Document each re-evaluation with a dated record noting what sources were checked and what was or was not found.

Detection Guidance

Because no CVE advisory or official indicator set exists, detection depends on behavioral hunting rather than signature matching.

Kubernetes API Server Audit Logs: Hunt for ClusterRoleBinding or RoleBinding creation events where the requesting user or service account is associated with the Azure Backup service rather than a Kubernetes-native admin identity. Any cluster-admin binding not traceable to an authorized change management record warrants immediate investigation. Look specifically for bindings created during periods of backup job execution.

Azure Activity Logs: Query for Azure Backup for AKS restore and configuration API calls. Flag operations initiated outside of scheduled backup windows or by identities that are not the designated backup service principal. Look for privilege escalation patterns: an identity invoking backup APIs that subsequently appears in Kubernetes audit logs with elevated permissions.

Kubernetes RBAC Drift: Compare current ClusterRoleBinding state against a known-good baseline. Any cluster-admin binding for an identity not in your approved list is a high-priority finding regardless of this specific vulnerability.

Azure AD / Entra ID Sign-In Logs: Review sign-in and access patterns for all identities holding the Backup Contributor role. Unusual access times, source IPs, or API call patterns warrant investigation.

Policy Gap Audit: Verify that Azure Policy or equivalent controls enforce least-privilege on Backup Contributor role assignments. If no scoping constraint exists, that is a control gap independent of whether exploitation occurred.

Log Retention Risk: The exposure window for this vulnerability is undefined. If your AKS audit log retention is less than 90 days, the relevant forensic window may already be lost. This is a prompt to review and extend retention policies for Kubernetes API server and Azure Activity Logs.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Azure Backup for AKS service identity / Backup Contributor role`	Azure Backup service identity leveraged via Confused Deputy mechanism — Backup Contributor role invoked backup APIs to cause the service's elevated trust context to act as a proxy, resulting in cluster-admin binding on targeted AKS clusters without direct Kubernetes permissions	HIGH
URL	`Pending — refer to BleepingComputer reporting (https://www.bleepingcomputer.com/news/security/microsoft-rejects-critical-azure-vulnerability-report-no-cve-issued/) for any indicators published by the original researcher`	Original researcher's disclosure may include specific API call sequences, permission validation bypass details, or proof-of-concept indicators not reproduced in available summary reporting	LOW

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism

- **T1098.003** — Additional Cloud Roles
- **T1078.004** — Cloud Accounts
- **T1530** — Data from Cloud Storage
- **T1610** — Deploy Container
- **T1134** — Access Token Manipulation

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **3.3** — Configure Data Access Control Lists
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1098.003	Additional Cloud Roles	Persistence
T1078.004	Cloud Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1610	Deploy Container	Defense-Evasion
T1134	Access Token Manipulation	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/microsoft-rejects-cr...	T3
Vulnerability management for Azure Kubernetes Service (AKS)	https://learn.microsoft.com/en-us/azure/aks/concepts-vulnerability-...	T1
Security bulletins for Azure Kubernetes Service (AKS)	https://learn.microsoft.com/en-us/azure/aks/security-bulletins/over...	T1
Azure Backup for AKS: Elevating Compliance and Cyber Resilience ...	https://techcommunity.microsoft.com/blog/azurestorageblog/azure-bac...	T1
Microsoft AKS best practices | TrendAI™ - Trend Micro	https://trendmicro.com/trendaivisiononecloudriskmanagement/knowledg...	T3

Generated 2026-05-17 13:50 UTC by TJS Security Command Center