INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-30 14:08 UTC

CVE-2026-26135: Azure Custom Locations Resource Provider Elevation of Privilege (Critical)

CVE VULNERABILITY | CRITICAL | CVSS 9.6

SCC Item ID	SCC-CVE-2026-0102
Type	CVE Vulnerability
CVE ID	CVE-2026-26135
Severity	CRITICAL
CVSS Base Score	9.6
EPSS Score	0.0005 (14th percentile)
Affected Products	Microsoft Azure Custom Locations Resource Provider (RP)
Published	2026-04-30T07:00:00
Discovery Source	Msrc Patch Tuesday

Executive Summary

Microsoft disclosed a critical elevation-of-privilege vulnerability (CVE-2026-26135, CVSS 9.6) in the Azure Custom Locations Resource Provider, part of the Azure Arc platform, during the April 2026 Patch Tuesday cycle. An attacker who has gained any foothold in an affected Azure environment can exploit this flaw to escalate privileges within the tenant or connected Kubernetes cluster scope. Organizations running Azure Arc-enabled Kubernetes deployments face the risk of unauthorized access to cloud resources, workloads, and sensitive configurations at elevated permission levels.

Technical Analysis

CVE-2026-26135 is a critical elevation of privilege (EoP) vulnerability in the Microsoft Azure Custom Locations Resource Provider (RP), an Azure Arc component that allows administrators to map Arc-enabled Kubernetes clusters as deployment targets for Azure services. The vulnerability is classified under CWE-269 (Improper Privilege Management) and maps to MITRE ATT&CK techniques T1548 (Abuse Elevation Control Mechanism) and T1078.004 (Valid Accounts: Cloud Accounts). CVSS base score is 9.6; CVSS vector is pending NVD publication. Precise attack vector mechanics and exploit prerequisites remain pending NVD enrichment and full MSRC advisory publication as of the configuration date. Exploitation requires an existing foothold or limited access within the affected Azure tenant or cluster; unauthenticated remote exploitation has not been confirmed.

No active exploitation (CISA KEV listing) has been recorded. EPSS score is 0.00047 (14th percentile), indicating low current exploitation probability, though the CVSS score warrants priority treatment given the blast radius of privilege escalation in cloud control-plane components. Full technical details should be retrieved directly from the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26135 and the NVD entry at https://nvd.nist.gov/vuln/detail/CVE-2026-26135 as enrichment becomes available. Note: These URLs are sourced from item data and should be validated by a human operator, as NVD enrichment and MSRC publication status may have changed since data ingestion.

Action Checklist

1. Containment: Identify all Azure subscriptions and tenants where Azure Arc is enabled and the Custom Locations Resource Provider is active. Review role assignments scoped to Custom Locations and restrict access to least-privilege principals immediately. Monitor the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26135 for patch availability and apply any Microsoft-released update to the Azure Custom Locations RP as soon as it is published.
2. Detection: Query Azure Activity Logs and Azure Arc resource logs for anomalous role assignments, unexpected privilege escalations, or unusual Custom Locations RP API calls (Microsoft.ExtendedLocation/* operations). Review Azure AD audit logs for account permission changes within Arc-connected scopes. Alert on any new Owner or Contributor assignments at the Custom Locations or connected cluster scope made outside approved change windows.
3. Eradication: Apply the Microsoft-released patch for CVE-2026-26135 to the Azure Custom Locations Resource Provider per the MSRC April 2026 guidance. Revoke any suspicious role assignments or access grants identified during detection. Rotate credentials for service principals associated with Custom Locations or Arc-enabled Kubernetes clusters if anomalous access is confirmed.
4. Recovery: Validate that the Custom Locations RP version running in affected subscriptions reflects the patched state per MSRC confirmation. Re-audit Azure RBAC assignments scoped to Custom Locations and Arc clusters post-remediation. Re-enable any temporarily restricted access only after patch validation. Monitor Azure Monitor and Defender for Cloud alerts for continued anomalous activity for a minimum of 14 days post-fix.
5. Post-Incident: Review Azure Arc deployment architecture for unnecessary Custom Locations RP exposure. Assess whether Kubernetes cluster RBAC and Azure RBAC policies enforce least-privilege adequately for Arc-connected workloads. Document any gaps in detection coverage for cloud control-plane privilege escalation and update threat hunting playbooks to include T1548 and T1078.004 patterns in Azure Arc environments.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if Azure Activity Logs confirm any successful `Microsoft.Authorization/roleAssignments/write` operations on Custom Locations or Arc-connected cluster scopes by non-approved principals during the exposure window, as this indicates confirmed exploitation of CVE-2026-26135 and potential unauthorized access to cloud-hosted data or infrastructure that may trigger breach notification obligations under applicable data protection regulations.

Recovery Notes	Validate the patched Custom Locations RP version against the specific build number cited in the MSRC April 2026 advisory — do not rely solely on `provisioningState: Succeeded` as confirmation of patch application. Re-enable any temporarily restricted Azure RBAC access only after both patch validation and a clean diff of pre- and post-remediation role assignment exports. Sustain elevated monitoring via Azure Monitor and Defender for Cloud alert rules scoped to `Microsoft.ExtendedLocation/*` and `Microsoft.Authorization/roleAssignments/*` events for a minimum of 14 days post-patch, specifically watching for T1078.004 patterns indicating an attacker attempting to re-establish access using credentials acquired during the exploitation window.
Forensic Artifacts	Azure Activity Logs — `Microsoft.ExtendedLocation/customLocations/*` and `Microsoft.Authorization/roleAssignments/write` operations: primary control-plane evidence of CVE-2026-26135 exploitation, showing attacker-inserted role assignments at the Custom Locations or Arc-connected cluster scope; retain 90-day export in JSON format with timestamps preserved. | Azure AD Audit Logs — `Add member to role` and `Add app role assignment` events scoped to service principals associated with Arc-connected Kubernetes clusters: evidence of identity-layer persistence established after privilege escalation via the Custom Locations RP vulnerability. | Kubernetes API server audit logs from Arc-connected clusters (`/var/log/kube-apiserver-audit.log` or EKS/AKS equivalents) — specifically `ClusterRoleBinding` and `RoleBinding` create/update events: evidence of lateral movement from Azure control-plane into connected cluster scope following CVE-2026-26135 exploitation. | Azure service principal sign-in logs (Microsoft Graph `auditLogs/signIns`) for Arc and Custom Locations RP service principals — filtered on sign-ins from unexpected IP ranges or applications: evidence of credential abuse by a threat actor who acquired service principal tokens after exploiting the elevation-of-privilege flaw. | Pre- and post-remediation RBAC snapshot diffs (`az role assignment list --all --output json`) scoped to Custom Locations and Arc cluster resources: definitive forensic record of which role assignments existed before containment, which were attacker-introduced, and which were revoked during eradication — required for both root cause determination and any regulatory breach notification analysis.

Per-Action IR Details

Containment — Identify all Azure subscriptions and tenants where Azure Arc is enabled and the Custom Locations Resource Provider is active. Review role assignments scoped to Custom Locations and restrict access to least-privilege principals immediately. Monitor the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26135 for patch availability and apply any Microsoft-released update to the Azure Custom Locations RP as soon as it is published.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: short-term containment to limit blast radius of privilege escalation across Azure Arc-connected scopes before patch availability

Controls: NIST IR-4 (Incident Handling), 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: Run `az account list --output table` to enumerate all subscriptions, then `az customlocation list --output table` per subscription to inventory active Custom Locations RPs. Execute `az role assignment list --all --query "[?contains(scope, 'customLocations')]" --output json` to dump scoped role assignments. For tenants without PAM tooling, manually export to CSV and diff against approved role baselines in your CMDB. Disable or restrict the Microsoft.ExtendedLocation resource provider registration via `az provider unregister --namespace Microsoft.ExtendedLocation` on non-essential subscriptions as a temporary measure.

Evidence: Before restricting any access, capture a full snapshot of current Azure RBAC state: export `az role assignment list --all --output json > rbac_snapshot_$(date +%Y%m%d).json` scoped to all Custom Locations

resources. Capture the Custom Locations RP version via `az customlocation show` output. Preserve Azure Activity Log entries for the 30-day window preceding discovery, filtering on `Microsoft.ExtendedLocation/*` operations and `Microsoft.Authorization/roleAssignments/write` events — these are the control-plane artifacts that will show whether CVE-2026-26135 was exploited to insert unauthorized role assignments prior to your containment action.

Detection — Query Azure Activity Logs and Azure Arc resource logs for anomalous role assignments, unexpected privilege escalations, or unusual Custom Locations RP API calls (Microsoft.ExtendedLocation/* operations). Review Azure AD audit logs for account permission changes within Arc-connected scopes. Alert on any new Owner or Contributor assignments at the Custom Locations or connected cluster scope made outside approved change windows.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlating cloud control-plane audit events across Azure Activity Logs, Azure AD, and Arc resource logs to identify indicators of privilege escalation via CVE-2026-26135

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

Compensating: Use Azure Monitor Log Analytics (free tier supports up to 5 GB/day) with this KQL query against AzureActivity: `AzureActivity | where OperationNameValue startswith 'Microsoft.ExtendedLocation' or OperationNameValue == 'Microsoft.Authorization/roleAssignments/write' | where ActivityStatusValue == 'Success' | where TimeGenerated > ago(30d) | project TimeGenerated, Caller, OperationNameValue, ResourceGroup, Properties`. For Azure AD audit logs, query `AuditLogs | where TargetResources has 'customlocation' or InitiatedBy has 'arc' | where TimeGenerated > ago(30d)`. Export results via `az monitor activity-log list --start-time 2026-03-01 --query "[?contains(operationName.value, 'ExtendedLocation')]" --output json` for offline analysis in a spreadsheet if Log Analytics is unavailable.

Evidence: Collect and preserve before analysis: Azure Activity Logs scoped to `Microsoft.ExtendedLocation/*` and `Microsoft.Authorization/roleAssignments/*` operations for the 30-day window; Azure AD audit log entries for `Add member to role` and `Add app role assignment` events associated with service principals linked to Arc-connected clusters; Kubernetes audit logs from Arc-connected clusters (located at `/var/log/kube-apiserver-audit.log` or via `kubectl get events -A --sort-by='.metadata.creationTimestamp'`) for unexpected ClusterRoleBinding or RoleBinding creation events that would indicate lateral movement from the Azure control plane into the connected cluster scope following exploitation of CVE-2026-26135.

Eradication — Apply the Microsoft-released patch for CVE-2026-26135 to the Azure Custom Locations Resource Provider per the MSRC April 2026 guidance. Revoke any suspicious role assignments or access grants identified during detection. Rotate credentials for service principals associated with Custom Locations or Arc-enabled Kubernetes clusters if anomalous access is confirmed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: removing the CVE-2026-26135 vulnerability from the Azure Custom Locations RP and purging attacker-established persistence via unauthorized role assignments and compromised service principal credentials

Controls: NIST SI-2 (Flaw Remediation), NIST IA-4 (Identifier Management), NIST AC-2 (Account Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For organizations without centralized patch orchestration, apply the MSRC-released Custom Locations RP update via `az extension update --name customlocation` or through the Azure Portal under the Arc | Custom Locations blade — verify the installed version matches the patched version cited in the MSRC April 2026 advisory. Revoke unauthorized role assignments with `az role assignment delete --ids `. Rotate service principal credentials using `az ad sp credential reset --id --append false` to force a full credential replacement rather than addition. For Arc-connected Kubernetes, audit and remediate ClusterRoleBindings with `kubectl get clusterrolebindings -o json | jq '.items[] | select(.subjects[].name | test("arc|customlocation"))'` and delete unauthorized bindings with `kubectl delete clusterrolebinding `.

Evidence: Before revoking any role assignments or rotating credentials, preserve: a JSON export of all suspicious role assignments flagged during detection (`az role assignment list --all --output json`); service principal sign-in logs from

Azure AD for the Arc-related service principals covering the exploitation window, exportable via Microsoft Graph API (`GET /auditLogs/signIns?$filter=appId eq '`); Kubernetes ClusterRoleBinding and RoleBinding manifests from Arc-connected clusters (`kubectl get clusterrolebindings,rolebindings -A -o yaml > k8s_rbac_snapshot.yaml`) to document attacker-inserted permissions that CVE-2026-26135 may have enabled within the connected cluster scope.

Recovery — Validate that the Custom Locations RP version running in affected subscriptions reflects the patched state per MSRC confirmation. Re-audit Azure RBAC assignments scoped to Custom Locations and Arc clusters post-remediation. Re-enable any temporarily restricted access only after patch validation. Monitor Azure Monitor and Defender for Cloud alerts for continued anomalous activity for a minimum of 14 days post-fix.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restoring Azure Arc-connected services to verified clean state, validating patch application, confirming RBAC integrity, and sustaining heightened monitoring for post-exploitation persistence attempts targeting Custom Locations RP

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Verify patched RP version with `az customlocation show --name --resource-group --query 'provisioningState'` and cross-reference the version string against the MSRC April 2026 advisory table. For the 14-day monitoring window without Defender for Cloud P2, configure an Azure Monitor Alert Rule on Activity Log events matching `Microsoft.ExtendedLocation/*` with action group paging on-call staff. Use `az monitor alert create` or the Portal. For Arc-connected Kubernetes, schedule a daily cron job running `kubectl get clusterrolebindings -o json | jq '.items[] | select(.metadata.creationTimestamp > "")' > /tmp/new_crb_$(date +%Y%m%d).json` to catch any new privileged bindings created after remediation.

Evidence: Capture post-remediation baseline artifacts to establish a known-good comparison state: re-export `az role assignment list --all --output json > rbac_post_remediation_$(date +%Y%m%d).json` and diff against the pre-containment snapshot to confirm all unauthorized assignments are purged; export Defender for Cloud security score and recommendations for the affected subscriptions; pull Kubernetes RBAC state post-cleanup (`kubectl get clusterrolebindings,rolebindings -A -o yaml > k8s_rbac_post_remediation.yaml`) as an integrity baseline. These artifacts serve as the chain-of-evidence anchor if any re-exploitation via CVE-2026-26135 or residual persistence is detected during the 14-day watch period.

Post-Incident — Review Azure Arc deployment architecture for unnecessary Custom Locations RP exposure. Assess whether Kubernetes cluster RBAC and Azure RBAC policies enforce least-privilege adequately for Arc-connected workloads. Document any gaps in detection coverage for cloud control-plane privilege escalation and update threat hunting playbooks to include T1548 and T1078.004 patterns in Azure Arc environments.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned review of Azure Arc architecture, RBAC posture gaps exposed by CVE-2026-26135, and detection engineering improvements for cloud control-plane privilege escalation targeting Arc-enabled Kubernetes

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Document detection gaps using a free MITRE ATT&CK Navigator layer (https://mitre-attack.github.io/attack-navigator/) — create a layer mapping T1548 (Abuse Elevation Control Mechanism) and T1078.004 (Valid Accounts: Cloud Accounts) to your current Azure log coverage, marking gaps in red. Develop a Sigma rule for the SIEM-agnostic detection of anomalous `Microsoft.ExtendedLocation/customLocations/write` and `Microsoft.Authorization/roleAssignments/write` co-occurrences within 5-minute windows (indicative of CVE-2026-26135 exploit chaining), exportable to Azure Sentinel, Splunk, or Elastic via the Sigma CLI converter (`sigmac -t rule.yml`). Archive the incident timeline, RBAC snapshots, and remediation evidence per NIST AU-11 (Audit

Record Retention) for a minimum retention period aligned to your policy.

Evidence: Assemble final post-incident evidence package: the complete timeline of `Microsoft.ExtendedLocation/*` and `Microsoft.Authorization/roleAssignments/*` Activity Log events from initial exposure window through eradication; before-and-after RBAC JSON snapshots demonstrating unauthorized assignment removal; Kubernetes audit log excerpts showing any ClusterRoleBinding anomalies tied to the Arc service principal during the incident window; and the MSRC advisory version confirmation output, all archived with SHA-256 checksums to preserve chain of custody for any regulatory inquiry triggered by unauthorized access to Arc-connected workloads.

Detection Guidance

Focus detection on the Azure control plane. Query Azure Activity Logs for Microsoft.ExtendedLocation resource provider operations, particularly role assignment writes (Microsoft.Authorization/roleAssignments/write) scoped to Custom Locations resources. In Microsoft Sentinel or your SIEM, alert on privilege escalation patterns: new Owner/Contributor/User Access Administrator assignments on Custom Locations or Arc-enabled Kubernetes cluster resources outside approved change windows. Review Azure Arc-enabled Kubernetes audit logs for unusual API server requests tied to elevated service accounts. Cross-reference with Azure AD sign-in logs for unexpected access from service principals associated with Custom Locations RP. Note: No public IOC signatures or specific exploit indicators have been published as of data ingestion; detection must rely on behavioral and RBAC anomaly patterns until MSRC technical details are enriched.

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1078.004** — Cloud Accounts

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings

OWASP-TOP10-2021

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

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **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
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1078.004	Cloud Accounts	Defense-Evasion

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26135	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-Apr	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33107	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32213	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33105	T1
CVE-2026-26135 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-26135	T1

Generated 2026-04-30 14:08 UTC by TJS Security Command Center