INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-18 18:50 UTC

# CVE-2026-42822: Azure Local Disconnected Operations (ALDO) Elevation of Privilege, CVSS 10.0 Critical

**CVE VULNERABILITY** | **CRITICAL** | CVSS 10.0

| | |
|---|---|
| **SCC Item ID** | SCC-CVE-2026-0190 |
| **Type** | CVE Vulnerability |
| **CVE ID** | CVE-2026-42822 |
| **Severity** | CRITICAL |
| **CVSS Base Score** | 10.0 |
| **Affected Products** | Microsoft Azure Local (Disconnected Operations / ALDO component); Azure Resource Manager (as reported in source data, exact product scope unconfirmed pending MSRC advisory review) |
| **Published** | 2026-05-18T07:00:00 |
| **Discovery Source** | Msrc Patch Tuesday |

## Executive Summary

Microsoft disclosed a CVSS 10.0 critical elevation of privilege vulnerability in Azure Local Disconnected Operations (ALDO) as part of the May 2026 Patch Tuesday release. A maximum CVSS score indicates the vulnerability is likely unauthenticated and remotely exploitable with no user interaction, allowing an attacker to gain full system control. Organizations running Azure Local in disconnected or hybrid edge deployments face the highest exposure and should treat this as an emergency patching event.

## Technical Analysis

CVE-2026-42822 is a critical elevation of privilege vulnerability in the Azure Local Disconnected Operations (ALDO) component, disclosed by Microsoft during the May 2026 Patch Tuesday cycle. The CVSS 10.0 base score indicates maximum impact across confidentiality, integrity, and availability. MITRE ATT&CK technique T1068 (Exploitation for Privilege Escalation) is mapped to this CVE. ALDO enables Azure Local instances to operate without continuous cloud connectivity, making edge and air-gapped deployments the primary at-risk environment. Specific attack vector, authentication requirements, exploit mechanics, and affected version ranges were not available in the source data at analysis time and could not be independently verified against MSRC or NVD. The vendor score and EPSS score fields are 0.0, indicating NVD and EPSS databases have not yet completed enrichment, this is expected for newly disclosed CVEs and does not reflect actual exploitability.

Azure Resource Manager is listed as potentially affected in source data but remains unconfirmed pending full MSRC advisory review. CWE classification was not available at time of analysis [pending NVD enrichment]. CISA KEV listing: not present as of analysis time. Primary references: MSRC Update Guide (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822), NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-42822), CVE Record (https://www.cve.org/CVERecord?id=CVE-2026-42822).

## Action Checklist

1. Step 1: Containment, Identify all Azure Local deployments running the ALDO (Disconnected Operations) component. Isolate affected nodes from lateral network paths where operationally feasible. Restrict administrative access to Azure Local management interfaces to known-good privileged access workstations while patching is staged. Consult the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822 to confirm affected build versions before any changes.
2. Step 2: Detection, Review Windows Security event logs on Azure Local nodes for anomalous privilege escalation events (Event IDs 4672, 4673, 4674, 4688 with unexpected high-privilege process creation). Query for T1068 indicators: unexpected processes running as SYSTEM or with elevated tokens, particularly in ALDO service contexts. Cross-reference with Azure Arc and Azure Monitor logs if cloud connectivity is available. No public IOCs or exploit signatures are available at this time.
3. Step 3: Eradication, Apply the Microsoft-issued patch from the May 2026 Patch Tuesday release cycle. Retrieve the specific KB article and update package from the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822). For disconnected environments, obtain the update package through your established offline update delivery mechanism. Do not defer patching pending EPSS enrichment; a CVSS 10.0 score warrants treatment as actively dangerous regardless of current exploit availability data.
4. Step 4: Recovery, After patching, verify the installed build version matches the remediated version specified in the MSRC advisory. Re-enable any isolated network paths in a staged manner with monitoring active. Confirm ALDO services restart cleanly and that disconnected operation functionality is intact. Review Azure Local activity logs for any anomalous privilege events in the 30 days prior to patching as a retroactive indicator sweep.
5. Step 5: Post-Incident, Evaluate your patch deployment SLA for critical infrastructure CVEs in disconnected environments; this vulnerability highlights the operational gap when air-gapped or ALDO-dependent nodes cannot receive updates through standard cloud-connected channels. Review whether privileged access to Azure Local management interfaces is appropriately segmented. Map this gap to NIST SP 800-53 controls SI-2 (Flaw Remediation) and CM-6 (Configuration Settings) and update your patch prioritization policy for edge deployments.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |

| | |
|---|---|
| **Escalation Criteria** | Escalate to full incident response (engage CISO, legal, and external IR retainer if applicable) immediately if the retroactive 30-day Event ID 4688 sweep or Azure Arc logs reveal any ALDO service host process spawning unexpected child processes with SYSTEM tokens, as this pattern indicates pre-patch exploitation and potentially undetected lateral movement or persistence within the Azure Local cluster; additionally, if Azure Local nodes are used to process regulated data (PII, PHI, PCI-DSS cardholder data, or federal CUI), a confirmed or suspected exploitation event triggers breach notification assessment obligations under applicable regulatory frameworks. |
| **Recovery Notes** | After patching all ALDO nodes to the MSRC-specified remediated build, maintain elevated monitoring on Windows Security Event IDs 4672, 4673, 4688, 7045, and 4697 for a minimum of 30 days to detect any persistence mechanisms (new services, scheduled tasks, or modified ALDO service binaries) installed during a potential pre-patch exploitation window. Re-enable isolated network paths in order of lowest-privilege segment first, verifying clean ALDO service operation and absence of anomalous outbound connections (particularly beaconing patterns on non-standard ports) at each stage before proceeding to the next. Retain all collected forensic artifacts — pre-patch binary hashes, event log exports, and netstat snapshots — for a minimum of 90 days in write-protected storage to support any retrospective investigation if exploitation evidence surfaces after recovery is declared complete. |
| **Forensic Artifacts** | Windows Security Event Log on each Azure Local node — specifically Event IDs 4688 (Process Creation) filtered for ALDO service host executables as parent processes and LOLBins (cmd.exe, powershell.exe, mshta.exe, wscript.exe) as child processes, representing the process spawn chain expected from a SYSTEM-level EoP exploit against an ALDO service context (MITRE ATT&CK T1068) \| ALDO service binary file hashes (SHA256) captured via Get-FileHash against the executable paths returned by 'Get-WmiObject Win32_Service \| Where-Object {$_.PathName -match "aldo"}' — pre- and post-patch comparison confirms whether binaries were tampered with or replaced during a potential exploitation window \| Registry export of HKLM\SYSTEM\CurrentControlSet\Services\ filtered for ALDO service entries — an attacker achieving SYSTEM via CVE-2026-42822 would likely modify service ImagePath, add a new service (Event ID 7045), or alter start type for persistence, all of which leave registry artifacts \| Azure Arc Connected Machine Agent logs at C:\ProgramData\AzureConnectedMachineAgent\Logs\ — post-exploitation abuse of Azure Arc's management plane (e.g., deploying malicious extensions or executing commands via Arc's RunCommand feature) would be logged here and represents the most likely lateral movement vector from a compromised Azure Local node to the broader Azure environment \| Windows crash dumps at C:\Windows\Minidump\ and C:\Windows\MEMORY.DMP predating the patch window — a CVSS 10.0 unauthenticated remote EoP exploit targeting an ALDO service may produce crash artifacts during failed or unstable exploitation attempts, and memory dump analysis can reveal injected shellcode, exploit heap spray patterns, or attacker-controlled memory regions not visible in event logs |

### Per-Action IR Details

**Step 1: Containment — Identify all Azure Local deployments running the ALDO (Disconnected Operations) component. Isolate affected nodes from lateral network paths where operationally feasible. Restrict administrative access to Azure Local management interfaces to known-good privileged access workstations while patching is staged. Consult the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822 to confirm affected build versions before any changes.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy

**Controls:** NIST IR-4 (Incident Handling), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** On each Azure Local node, run 'Get-AzureStackHCI' (PowerShell) to enumerate ALDO component version and confirm affected build. Use Windows Firewall ('netsh advfirewall' or PowerShell Set-NetFirewallProfile) to block inbound connections on management ports (WinRM TCP 5985/5986, RDP TCP 3389) from all sources except designated PAW IP addresses. For nodes without remote management capability, physically restrict KVM or console access. Document all affected node hostnames, build versions, and network segment assignments before any isolation action.

**Evidence:** Before isolating any node, capture: (1) a full netstat -ano output to record active connections into Azure Local management interfaces at time of discovery; (2) a snapshot of running services via 'Get-Service | Where-Object {$_.Status -eq "Running"}' filtered for ALDO-related service names; (3) Windows Security Event Log export covering the 30 days prior, filtering on Event IDs 4672 (Special Privilege Logon), 4673 (Privileged Service Called), and 4624 (Logon) for Type 3 (network) and Type 10 (remote interactive) logons to Azure Local management accounts — these would capture any pre-containment exploitation of the unauthenticated EoP path.

**Step 2: Detection — Review Windows Security event logs on Azure Local nodes for anomalous privilege escalation events (Event IDs 4672, 4673, 4674, 4688 with unexpected high-privilege process creation). Query for T1068 indicators: unexpected processes running as SYSTEM or with elevated tokens, particularly in ALDO service contexts. Cross-reference with Azure Arc and Azure Monitor logs if cloud connectivity is available. No public IOCs or exploit signatures are available at this time.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis

**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:** Deploy Sysmon (with SwiftOnSecurity or Olaf Hartong config) on all Azure Local nodes if not already present — Event ID 1 (Process Create) will capture parent-child process relationships for any process spawned by ALDO service hosts (look for unexpected cmd.exe, powershell.exe, or wscript.exe children of ALDO service processes). Use the following PowerShell query against the Security event log: 'Get-WinEvent -LogName Security -FilterXPath "*[System[(EventID=4688)]]" | Where-Object {$_.Properties[8].Value -match "SYSTEM" -and $_.Properties[5].Value -notmatch ""}'. For Azure Arc-connected nodes, query Azure Monitor Log Analytics with: 'SecurityEvent | where EventID in (4672,4688) | where SubjectUserName !in ("SYSTEM","") | project TimeGenerated, Computer, EventID, SubjectUserName, ProcessName'.

**Evidence:** Capture before analysis: (1) Sysmon Event ID 1 logs showing process lineage from ALDO service host processes (identify ALDO service executable names from 'Get-WmiObject Win32_Service | Where-Object {$_.PathName -match "aldo"}' output); (2) Windows Security Event ID 4688 (Process Creation) entries with 'Creator Process Name' matching ALDO service executables and 'New Process Name' showing cmd.exe, powershell.exe, mshta.exe, or other LOLBins — this process injection or spawn chain is the expected artifact of a SYSTEM-level EoP exploit targeting a service context (MITRE ATT&CK T1068); (3) Azure Arc agent logs at C:\ProgramData\AzureConnectedMachineAgent\Logs\ for anomalous API calls or policy application events that could indicate post-exploitation use of Arc's management plane; (4) Windows Event ID 7045 (New Service Installed) and 4697 (Service Installed) for any persistence mechanism installed after privilege escalation.

**Step 3: Eradication — Apply the Microsoft-issued patch from the May 2026 Patch Tuesday release cycle. Retrieve the specific KB article and update package from the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822). For disconnected environments, obtain the update package through your established offline update delivery mechanism. Do not defer patching pending EPSS enrichment — a CVSS 10.0 score warrants treatment as actively dangerous regardless of current exploit availability data.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST SA-10 (Developer Configuration Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

**Compensating:** For ALDO disconnected environments without WSUS or cloud update access: use the Azure Local LCM (Lifecycle Manager) offline update workflow — stage the KB package on a local SMB share accessible to the cluster, then invoke 'Invoke-AzStackHCISolutionUpdate' with the local path parameter. Verify the KB number from the MSRC advisory matches the staged package using 'Get-FileHash' (SHA256) against the MSRC-published hash before deployment. After patching, run 'Get-AzureStackHCIUpdateSummary' to confirm installed version. If LCM is unavailable, apply via 'Add-WindowsPackage' (DISM) or 'wusa.exe .msu /quiet /norestart' and manually verify with 'Get-HotFix -Id KB'.

**Evidence:** Before applying the patch, capture a system state snapshot: (1) export the current ALDO service binary file hashes using 'Get-FileHash -Path (Get-WmiObject Win32_Service | Where-Object {$_.PathName -match "aldo"}).PathName' — these pre-patch hashes establish a baseline and can confirm whether an attacker replaced or modified ALDO binaries prior to your patching event; (2) export the registry key 'HKLM\SYSTEM\CurrentControlSet\Services\' filtered for ALDO service entries to capture any tampering with service ImagePath or start type that would indicate post-exploitation persistence; (3) collect any crash dumps from C:\Windows\Minidump\ or C:\Windows\MEMORY.DMP that pre-date the patch window — exploitation of a CVSS 10.0 service-level EoP can produce crash artifacts if the exploit path involved memory corruption or unstable privilege transitions.

**Step 4: Recovery — After patching, verify the installed build version matches the remediated version specified in the MSRC advisory. Re-enable any isolated network paths in a staged manner with monitoring active. Confirm ALDO services restart cleanly and that disconnected operation functionality is intact. Review Azure Local activity logs for any anomalous privilege events in the 30 days prior to patching as a retroactive indicator sweep.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** Verify patch integrity post-install using 'Get-HotFix' and cross-reference the KB number against the MSRC advisory build table. Use Sysmon Event ID 7 (Image Loaded) combined with a YARA rule targeting the vulnerable ALDO component DLL/EXE to confirm the patched version is loaded at runtime — the YARA rule should key on the file version metadata field matching the remediated build. For the retroactive 30-day sweep without a SIEM: run the PowerShell query 'Get-WinEvent -LogName Security -MaxEvents 50000 | Where-Object {$_.Id -in @(4672,4673,4674,4688) -and $_.TimeCreated -gt (Get-Date).AddDays(-30)}' exported to CSV and filtered for ALDO service account names and SYSTEM-level token assignments occurring outside scheduled maintenance windows.

**Evidence:** During recovery validation, collect: (1) 'Get-AzureStackHCIUpdateSummary' output showing installed KB and build version matching the MSRC-specified remediated release — screenshot or export this as documented evidence of patch application; (2) Windows System Event Log Event ID 7036 (Service State Change) for ALDO services confirming clean start post-patch, and Event ID 7031 (Service Terminated Unexpectedly) confirming absence of crash loops that could indicate an incomplete or failed patch application; (3) a second pass of the 30-day retroactive Event ID 4688 sweep with parent process filtering for ALDO service hosts — any hits here represent potential pre-patch exploitation activity requiring escalation to a full forensic investigation rather than routine recovery.

**Step 5: Post-Incident — Evaluate your patch deployment SLA for critical infrastructure CVEs in disconnected environments — this vulnerability highlights the operational gap when air-gapped or ALDO-dependent nodes cannot receive updates through standard cloud-connected channels. Review whether privileged access to Azure Local management interfaces is appropriately segmented. Map this gap to NIST SP 800-53 controls SI-2 (Flaw Remediation) and CM-6 (Configuration Settings) and update your patch prioritization policy for edge deployments.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity

**Controls:** NIST SI-2 (Flaw Remediation), NIST CM-6 (Configuration Settings), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

**Compensating:** Document the gap analysis in a structured lessons-learned format: record the time-delta between MSRC disclosure (May 2026 Patch Tuesday) and patch application on each ALDO node, and compare against your defined SLA for CVSS 10.0 CVEs. If no SLA exists for disconnected/edge nodes, draft one using CIS 7.2 as the framework — recommend a 72-hour emergency patch window for CVSS 9.0+ vulnerabilities affecting internet-edge or management-plane components regardless of connectivity tier. Use osquery ('SELECT * FROM patches WHERE hotfix_id LIKE "KB%"') scheduled as a weekly cron job across all Azure Local nodes to maintain a live patch-state inventory that flags ALDO component build versions against your approved baseline, providing an ongoing detection capability for future ALDO-category advisories.

**Evidence:** Post-incident documentation should capture: (1) a complete timeline reconstructed from Windows Security Event Log and Azure Arc agent logs showing the window between MSRC disclosure and confirmed patch application on each ALDO node — this timeline is the primary evidence for SLA compliance review and regulatory reporting if required; (2) the output of 'Get-AzureStackHCIUpdateSummary' from every affected node as proof-of-remediation artifacts to be retained per NIST AU-11 (Audit Record Retention) requirements for your organization's defined retention period; (3) documented confirmation that no Event ID 4688 parent-ALDO-process-to-SYSTEM-child entries were identified in the retroactive 30-day sweep — if any were found, this post-incident step must be re-classified as an active breach investigation and escalated accordingly.

## Detection Guidance

No public exploit code, IOCs, or behavioral signatures specific to CVE-2026-42822 are available at this time. Detection should focus on host-level privilege escalation indicators on Azure Local nodes. Monitor Windows Security event logs for: Event ID 4672 (special privileges assigned to new logon), Event ID 4688 (process creation with elevated tokens, particularly unexpected SYSTEM-context processes), and Event ID 7045 (new service installed). Correlate against ALDO service process trees for anomalous child process spawning. If Azure Monitor or Microsoft Sentinel is available, query for unusual privileged activity on Azure Local cluster nodes during the window between patch availability and patch deployment. Update endpoint detection rules to include T1068 (Exploitation for Privilege Escalation) behavioral patterns in Azure Local service contexts. Once the MSRC advisory publishes full technical details, revisit detection logic with vendor-provided indicators.

## Framework Mappings

### MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation

### NIST-800-53R5

- **AC-6** — Least Privilege
- **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
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

**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 |
|---|---|---|
| T1068 | Exploitation for Privilege Escalation | Privilege-Escalation |

## Sources

| Source | URL | Tier |
|---|---|---|
| **MSRC Update Guide** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42822 | T1 |
| **(consolidated)** | https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May | T1 |
| **CVE-2026-4282 Detail - NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-4282 | T1 |
| **CVE-2026-42822 - CVE Record** | https://www.cve.org/CVERecord?id=CVE-2026-42822 | T3 |
| **CVE-2026-42826 Detail - NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-42826 | T1 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-42822 | T1 |



Generated 2026-05-18 18:50 UTC by TJS Security Command Center