INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:24 UTC

AI-Driven Vulnerability Discovery Is Reshaping Patch Tuesday, And Your Patch Cadence Must Keep Up

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0185
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows, Microsoft on-premises software, Microsoft PaaS and SaaS cloud services
Published	2026-06-09T18:07:28
Discovery Source	Rss

Executive Summary

Microsoft MSRC has acknowledged that AI-assisted vulnerability scanning is directly driving a measurable increase in Patch Tuesday volume, with May 2026 releases reflecting accelerated discovery velocity. This is not a temporary spike; it reflects a permanent acceleration in discovery speed as external researchers deploy AI tooling at scale, narrowing the window between vulnerability existence and public disclosure. Organizations still operating on monthly patch cadences or annual risk-tolerance reviews are now structurally exposed: the gap between disclosure and exploitation is narrowing faster than traditional programs were designed to respond to.

Technical Analysis

Analysis from Microsoft MSRC and security researchers indicates that AI-assisted vulnerability discovery is driving a structural shift in disclosure velocity, not a temporary cycle. AI-assisted scanning tools are enabling researchers, both internal teams and independent external actors, to identify vulnerability patterns across large codebases at a speed and breadth that human-led analysis cannot match. The result is an expanding disclosure surface that cuts across multiple CWE categories simultaneously: improper input validation (CWE-20), memory buffer errors (CWE-119), use-after-free conditions (CWE-416), and improper privilege management (CWE-269). This spread across multiple CWE categories suggests that AI-assisted discovery is flagging diverse weakness patterns, not a single class of vulnerability.

The MITRE ATT&CK techniques associated with this disclosure cluster tell the exploitation story: T1190 (Exploit Public-Facing Application), T1210 (Exploitation of Remote Services), T1203 (Exploitation for Client Execution),

and T1068 (Exploitation for Privilege Escalation). Together, these represent initial access, lateral movement, and privilege escalation, a near-complete kill chain built from disclosed vulnerabilities. An adversary who patches faster than a defender exploits a structural lag that monthly cadences were never designed to close.

The affected surface spans Microsoft Windows, on-premises software, and PaaS and SaaS cloud services, which introduces a shared-responsibility dimension. For cloud-hosted workloads, Microsoft carries patching responsibility for the underlying platform (per Azure shared responsibility documentation). However, OS-layer and application-layer components in IaaS environments, and all on-premises deployments, remain the customer's responsibility. Organizations that have not mapped their asset inventory against that responsibility boundary may be carrying silent exposure they believe is covered.

The practical implication for vulnerability management programs is a forced re-examination of SLA definitions tied to monthly patching cycles. If AI tooling enables discovery of dozens of high-severity vulnerabilities in a single release cycle, with exploitation-relevant techniques already publicly mapped, a 30-day remediation SLA for critical findings is no longer a defensible standard for high-exposure assets. Programs must stratify: continuous patching workflows for internet-facing and privilege-relevant systems, risk-accepted deferral processes with compensating controls for lower-exposure internal assets, and updated threat models that treat AI-accelerated disclosure as a baseline condition rather than an exception.

Action Checklist

1. Step 1: Assess exposure, audit your inventory for all Microsoft Windows, Microsoft on-premises software, and Microsoft PaaS/SaaS services; map each asset against the Azure shared-responsibility model to confirm who holds patching accountability for each layer (reference CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory)
2. Step 2: Review patch SLAs, evaluate whether your current remediation SLAs (commonly 30/60/90 days by severity) remain defensible given accelerated disclosure velocity; prioritize assets exposed to T1190 (Exploit Public-Facing Application) and T1068 (Exploitation for Privilege Escalation) for immediate SLA tightening
3. Step 3: Triage by CWE and technique, cross-reference May 2026 Patch Tuesday disclosures against your asset inventory for CWE-20, CWE-119, CWE-416, and CWE-269; flag any unpatched findings that map to T1210 or T1203 as elevated-priority given client-execution and remote-service exploitation potential
4. Step 4: Validate compensating controls, for assets where patching cannot be immediate, verify compensating controls are in place: least-privilege enforcement (NIST AC-6), input validation at application boundaries, memory integrity protections, and privilege management reviews (NIST AC-5: Separation of Duties); apply NIST AC-2 (Account Management) and NIST AC-6 (Least Privilege) to enforce privilege boundaries and credential controls
5. Step 5: Update vulnerability management policy, revise your vulnerability management policy to classify AI-accelerated discovery as a standing operating condition; introduce a continuous patching tier for internet-facing and high-privilege assets separate from the standard monthly cadence (reference CIS 7.1: Establish and Maintain a Vulnerability Management Process and CIS 7.2: Establish and Maintain a Remediation Process)
6. Step 6: Monitor for exploitation activity, establish detection coverage for the four mapped ATT&CK techniques; watch for anomalous privilege escalation events, exploitation attempts against public-facing services, and client-execution patterns in endpoint telemetry (reference NIST AU-6: Audit Record Review,

Analysis, and Reporting)

7. Step 7: Brief leadership, communicate to executive leadership that Patch Tuesday volumes are increasing as a direct result of AI tooling adoption in the researcher community, and that maintaining current patch cadence without adjustment represents a widening and measurable exploitation window

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident response engagement if Sysmon or Windows Event Log detection queries (T1190, T1068, T1210, T1203) produce confirmed hits against unpatched Microsoft assets, if any internet-facing asset running unpatched May 2026 Patch Tuesday vulnerabilities shows anomalous outbound connections or unexpected privilege escalation events, or if the organization's MTTP for Critical Microsoft patches exceeds 30 days and internet-facing assets are confirmed unpatched — at which point regulatory breach notification timelines (GDPR 72-hour, HIPAA 60-day, SEC 4-day material incident) may be triggered depending on asset data classification.
Recovery Notes	After patching Microsoft Windows and on-premises software assets, verify patch application by re-running 'wmic qfe list full' and comparing against the Step 1 baseline CSV to confirm all May 2026 Patch Tuesday CVEs are reflected; re-run the Sysmon and Windows Event Log detection queries established in Step 6 for a minimum of 14 days post-patch to confirm no exploitation activity occurred in the gap period and no persistence mechanisms (scheduled tasks, registry run keys, new local admin accounts) were established during the window of exposure. For Azure PaaS and SaaS services where Microsoft holds patching accountability, verify remediation status through Azure Security Center / Microsoft Defender for Cloud 'Recommendations' blade and retain a dated export as evidence that the shared-responsibility boundary was monitored.

Forensic Artifacts	Windows Error Reporting crash dumps at '%ProgramData%\Microsoft\Windows\WER\ReportArchive\' — CWE-119 (buffer overflow) and CWE-416 (use-after-free) memory corruption exploits against Windows kernel or GDI components frequently generate WER reports before or during exploitation; these are time-stamped and persist across reboots, making them high-value pre-exploitation indicators specific to memory corruption CVE classes in May 2026 Patch Tuesday | IIS access logs at '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' — T1190 exploitation attempts against Microsoft on-premises web services (IIS, Exchange OWA, SharePoint) leave URI patterns, HTTP verb anomalies, and error code spikes (HTTP 500, 400 series) that are absent from normal traffic; CWE-20 (improper input validation) exploits in particular produce malformed or oversized request bodies visible in W3C extended log format | Windows Security Event Log Event ID 4688 (Process Creation with command line) — T1068 privilege escalation exploits targeting unpatched Windows services or kernel vulnerabilities frequently result in unexpected high-privilege process spawning; filter for processes where the parent is a Microsoft service executable (svchost.exe, lsass.exe, spoolsv.exe) and the child is cmd.exe, PowerShell, or a renamed shell, which is the post-exploitation pattern for CWE-269 privilege management flaws | Microsoft Office Protected View and macro execution logs in the Windows Application Event Log (Event Source: Microsoft Office Alerts) combined with Sysmon Event ID 1 parent-child process chains — T1203 client execution exploits delivered via malicious Office documents or browser-rendered content targeting CWE-119/CWE-416 vulnerabilities in Microsoft rendering engines leave parent-child process anomalies (WINWORD.EXE or MSEDGE.EXE spawning PowerShell or wscript.exe) that are directly attributable to document-borne exploitation rather than user-initiated activity | Azure Activity Log and Microsoft Entra ID (formerly Azure AD) Sign-In Logs accessible via Azure Monitor — for Microsoft PaaS and SaaS cloud services within scope, post-exploitation lateral movement and privilege escalation (T1068 in cloud context) produce anomalous role assignment events (operationName: 'Microsoft.Authorization/roleAssignments/write'), impossible-travel sign-in alerts, and service principal credential additions that are specific to cloud-layer exploitation and distinct from on-premises artifact sets

Per-Action IR Details

Step 1: Assess exposure — audit your inventory for all Microsoft Windows, Microsoft on-premises software, and Microsoft PaaS/SaaS services; map each asset against the Azure shared-responsibility model to confirm who holds patching accountability for each layer (reference CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and asset visibility before incidents occur

Controls: CIS 1.1 (IG1/IG2/IG3) — Establish and Maintain Detailed Enterprise Asset Inventory, NIST AC-20 — Use Of External Systems

Compensating: Run 'Get-WindowsUpdateLog' via PowerShell on Windows hosts to surface patch state per machine; enumerate Azure resources without licensing cost using Azure Resource Graph Explorer (free, built into Azure Portal) with query: 'Resources | project name, type, location, properties.provisioningState' to identify PaaS/SaaS assets where Microsoft holds patching responsibility versus IaaS where the organization does. For on-premises, use the free Microsoft Baseline Security Analyzer successor — 'winget install Microsoft.SecurityCompliance' — or export from WSUS console if deployed.

Evidence: Before remediating any asset, snapshot current patch state: capture output of 'wmic qfe list full /format:csv > patch_inventory_YYYYMMDD.csv' per host; export Azure Advisor 'Security' recommendations to CSV from the portal to document which Azure-managed layers had known gaps at time of assessment; preserve WSUS/Windows Update client logs at '%SystemRoot%\SoftwareDistribution\ReportingEvents.log' to establish a pre-remediation baseline for later comparison.

Step 2: Review patch SLAs — evaluate whether your current remediation SLAs (commonly 30/60/90 days by severity) remain defensible given accelerated disclosure velocity; prioritize assets exposed to T1190 (Exploit Public-Facing Application) and T1068 (Exploitation for Privilege Escalation) for immediate SLA tightening

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Policy and procedure readiness to respond to a changed threat landscape

Controls: CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process

Compensating: Build a free SLA tracking spreadsheet cross-referenced to Microsoft's MSRC severity ratings (Critical/Important/Moderate/Low) and tag each row with T1190 or T1068 exposure based on whether the asset is internet-facing or runs a privileged service; set a calendar-triggered PowerShell script using Task Scheduler to query 'Get-HotFix | Where-Object {$_.InstalledOn -lt (Get-Date).AddDays(-14)}' and email results to the security team, providing a no-cost SLA breach alert for any patch older than your tightened window.

Evidence: Document the current SLA policy version and approval date before revising it; export the last 90 days of Microsoft Security Update Guide data (downloadable as JSON from https://api.msrc.microsoft.com/cvrf/v3.0/updates — label as search-verified, recommend human validation) to quantify the disclosure velocity increase; preserve a snapshot of any existing risk-acceptance records for delayed patches on T1190-exposed assets, as these become evidence of pre-revision risk posture if exploitation occurs.

Step 3: Triage by CWE and technique — cross-reference May 2026 Patch Tuesday disclosures against your asset inventory for CWE-20, CWE-119, CWE-416, and CWE-269; flag any unpatched findings that map to T1210 or T1203 as elevated-priority given client-execution and remote-service exploitation potential

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlating vulnerability disclosures against asset inventory to assess scope and severity

Controls: CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 2.2 (IG1/IG2/IG3) — Ensure Authorized Software is Currently Supported

Compensating: Download the May 2026 MSRC CVRF feed and parse CWE tags using a free Python script with 'requests' and 'xml.etree.ElementTree' to filter for CWE-20 (Improper Input Validation), CWE-119 (Buffer Errors), CWE-416 (Use-After-Free), and CWE-269 (Improper Privilege Management) entries; cross-reference resulting CVE list against your asset inventory CSV from Step 1 using a simple 'vlookup' or 'pandas merge'; for T1203-mapped findings specifically, enumerate all Microsoft Office, browser, and PDF reader versions on endpoints using 'winget list --source winget' output piped to a file for offline comparison.

Evidence: For CWE-119 and CWE-416 (memory corruption classes common in Windows kernel and GDI components), capture Windows Error Reporting crash dumps at '%ProgramData%\Microsoft\Windows\WER\ReportArchive\' — these predate exploitation and establish a no-exploitation baseline; for CWE-269 privilege management weaknesses, export current local group membership via 'Get-LocalGroupMember -Group Administrators | Export-Csv admins_baseline.csv' before any changes; for T1203-exposed assets (client execution via document/file exploitation), note which users have opened email attachments or downloaded files in the 30 days prior by reviewing Exchange message tracking logs or Outlook sent/received folder metadata.

Step 4: Validate compensating controls — for assets where patching cannot be immediate, verify compensating controls are in place: least-privilege enforcement (NIST AC-6), input validation at application boundaries, memory integrity protections, and privilege management reviews (NIST AC-5: Separation of Duties); apply D3-UAP (User Account Permissions) and D3-CH (Credential Hardening) where privilege escalation paths are exposed

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Implementing controls to limit exploitation impact while full remediation is pending

Controls: NIST AC-6 — Least Privilege, NIST AC-5 — Separation Of Duties, CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts

Compensating: Enable Windows Defender Credential Guard via Group Policy (Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security) at no cost to harden against T1068 privilege escalation on unpatched hosts; deploy Sysmon with the SwiftOnSecurity config (free, GitHub-hosted) and enable Event ID 8 (CreateRemoteThread) and Event ID 10 (ProcessAccess) to detect in-memory privilege escalation attempts characteristic of CWE-269 exploits against unpatched Windows services; run 'secedit /export /cfg current_policy.cfg' to snapshot current security policy before any compensating control changes.

Evidence: Before applying compensating controls, capture a process privilege snapshot using 'Get-Process | Select-Object Name, Id, @{N="User";E={$_.GetOwner().User}} | Export-Csv process_privs_before.csv'; export current Windows token privilege assignments via 'whoami /priv' on all service accounts running vulnerable on-premises Microsoft software; document existing Windows Defender Application Guard, WDAC, or AppLocker policy status via 'Get-AppLockerPolicy -Effective | Export-Clixml applocker_state.xml' to confirm memory integrity and execution controls state prior to any modifications.

Step 5: Update vulnerability management policy — revise your vulnerability management policy to classify AI-accelerated discovery as a standing operating condition; introduce a continuous patching tier for internet-facing and high-privilege assets separate from the standard monthly cadence (reference CIS 7.1: Establish and Maintain a Vulnerability Management Process and CIS 7.2: Establish and Maintain a Remediation Process)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned and policy updates driven by changed threat conditions

Controls: CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process, NIST AC-1 — Policy And Procedures

Compensating: Document the new continuous patching tier in a one-page policy addendum that defines the trigger condition (any Critical Microsoft patch touching an internet-facing asset or a T1190/T1068-mapped CVE) and the target remediation window (72 hours from MSRC release); automate detection of new Patch Tuesday releases by subscribing to the MSRC Security Update Guide RSS feed and routing it to a shared email alias or free Slack webhook so the 2-person team is notified within hours of release rather than days.

Evidence: Preserve the prior policy version with its effective date and last-approval signature before revision — this establishes a documented record of when the organization formally recognized AI-accelerated disclosure as a standing condition, which is relevant to regulatory defensibility; archive the May 2026 Patch Tuesday MSRC release metadata (CVE count, hotpatch count, severity distribution) as the evidentiary basis for the policy change, citing it explicitly in the policy revision history.

Step 6: Monitor for exploitation activity — establish detection coverage for the four mapped ATT&CK techniques; watch for anomalous privilege escalation events, exploitation attempts against public-facing services, and client-execution patterns in endpoint telemetry (reference NIST AU-6: Audit Record Review, Analysis, and Reporting)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring and correlation to identify exploitation of unpatched Microsoft vulnerabilities

Controls: NIST AU-6 — Audit Record Review, Analysis, And Reporting, NIST AU-2 — Event Logging, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Deploy the following Sysmon + Windows Event Log queries for each ATT&CK technique: T1190 — query IIS logs at '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' for HTTP 500 responses and anomalous URI patterns (encoded payloads, path traversal strings) using 'Select-String -Path "*.log" -Pattern "(%2e|%2f|cmd.exe|powershell)"'; T1068 — Windows Security Event ID 4672 (Special Privileges Assigned to New

Logon) and Sysmon Event ID 8 (CreateRemoteThread) where source process is a Microsoft service executable; T1210 — Windows Security Event ID 4624/4625 with logon type 3 (network) from unexpected sources targeting SMB or RPC ports; T1203 — Sysmon Event ID 1 (Process Create) where parent is a Microsoft Office application (WINWORD.EXE, EXCEL.EXE) spawning cmd.exe, PowerShell, or wscript.exe. All four can be implemented as free Sigma rules converted to PowerShell queries using the Sigma CLI tool.

Evidence: Before establishing detection baselines, export 30 days of Windows Security Event Log (Event IDs 4624, 4625, 4648, 4672, 4688) using 'wevtutil epl Security security_baseline.evtx'; capture current IIS and Windows Application Event Log state for all internet-facing Microsoft on-premises services as a pre-exploitation reference; snapshot active network connections on public-facing assets using 'netstat -ano | Out-File netstat_baseline_YYYYMMDD.txt' to establish normal connection profiles against which anomalous post-exploitation lateral movement (T1210) can be compared.

Step 7: Brief leadership — communicate to executive leadership that Patch Tuesday volumes are increasing as a direct result of AI tooling adoption in the researcher community, and that maintaining current patch cadence without adjustment represents a widening and measurable exploitation window

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Ensuring organizational leadership supports and resources the IR capability required to respond to an accelerated threat environment

Controls: NIST AC-1 — Policy And Procedures

Compensating: Prepare a one-page executive brief using concrete metrics: pull the trailing 12-month Patch Tuesday CVE count from MSRC (filterable by product family — Windows, on-premises server, cloud services) and show the trend line; calculate the current mean-time-to-patch (MTTP) for your environment from the Step 1 patch inventory CSV versus the new AI-compressed disclosure-to-exploit window (publicly documented by MSRC in their May 2026 advisory); frame the risk as a gap metric — days of exposure = days since MSRC release minus days to patch — and show how that gap widens under current cadence as disclosure velocity increases.

Evidence: Attach the patch inventory export from Step 1 and the SLA review output from Step 2 as supporting exhibits; document any current open risk acceptances for Critical or Important Microsoft patches beyond 30 days on internet-facing assets — these represent the measurable exploitation window the brief references and should be listed by asset tier, not individual CVE, to keep the brief executive-appropriate without exposing operational detail in a non-secure briefing context.

Detection Guidance

Detection for this story centers on exploitation of the four ATT&CK techniques rather than specific IOCs, since no campaign-specific indicators have been published. As of publication, no confirmed exploitation campaigns targeting May 2026 Patch Tuesday disclosures have been published. Organizations should establish detection baselines for the listed techniques in advance of potential exploitation activity.

For T1190 and T1210 (public-facing and remote service exploitation): Review WAF and perimeter logs for anomalous request patterns targeting Microsoft IIS, Exchange, SharePoint, or RDP endpoints, particularly malformed inputs consistent with CWE-20 exploitation attempts. Correlate web server access logs with upstream proxy logs for request anomalies.

For T1068 (privilege escalation): Hunt for processes spawning with elevated privileges from unexpected parent processes, token manipulation events in Windows Security event logs (Event IDs 4672, 4673, 4674), and sudden changes to local administrator group membership. CWE-269 (improper privilege management) and CWE-416 (use-after-free) exploitation frequently manifests as unexpected SYSTEM-level process creation. Apply NIST AC-2 (Account Management) and Windows Security event log monitoring (Event IDs 4732, 4733) to surface anomalous local privilege changes.

For T1203 (client execution exploitation): Monitor for Office process spawning child processes (especially cmd.exe, PowerShell, or wscript.exe), browser renderer process anomalies, and document execution chains outside expected application behavior. CWE-119 (buffer errors) and CWE-416 exploitation in client applications often produces crash telemetry before successful exploitation, review Windows Error Reporting logs and application crash data for patterns.

Audit gaps to check: Verify that NIST AU-2 (Event Logging) covers privilege escalation events and process creation on all Windows endpoints. Confirm NIST AU-12 (Audit Record Generation) is enabled for authentication and process execution. Review CIS 8.2 (Collect Audit Logs) compliance across your Windows estate, gaps in log collection are the most common reason exploitation goes undetected until post-incident.

For cloud assets: Review Azure Activity Logs and Microsoft Defender for Cloud alerts for anomalous API calls, privilege assignments, or resource modification events on PaaS services.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1203** — Exploitation for Client Execution
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **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.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1210	Exploitation of Remote Services	Lateral-Movement
T1190	Exploit Public-Facing Application	Initial-Access
T1203	Exploitation for Client Execution	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://www.microsoft.com/en-us/msrc/blog/2026/05/a-note-on-patch-t...	T1
Shared responsibility in the cloud - Azure - Microsoft Learn	https://learn.microsoft.com/en-us/azure/security/fundamentals/share...	T1
Best practices for secure PaaS deployments - Azure - Microsoft Learn	https://learn.microsoft.com/en-us/azure/security/fundamentals/paas-...	T1
Azure Cloud Security: The Critical Vulnerabilities You're ... - Intruder.io	https://www.intruder.io/blog/azure-cloud-security	T3
Introduction to Azure security | Microsoft Learn	https://learn.microsoft.com/en-us/azure/security/fundamentals/overview	T1

Generated 2026-06-10 07:24 UTC by TJS Security Command Center