INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:36 UTC

UAT-8302: China-Nexus APT Shares Tooling Across Multiple Clusters to Target Government Networks on Three Continents

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0273
Type	Threat Campaign
CVE ID	CVE-2025-0994
Severity	HIGH
CVSS Base Score	9.5
EPSS Score	0.7486 (99th percentile)
Affected Products	Government networks in South America and southeastern Europe; Microsoft OneDrive and MS Graph API (abused for C2); Microsoft Active Directory; Azure AD Connect / Entra ID Connect; MobaXterm; Windows endpoints in government environments
Published	2026-05-05T10:00:30+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Cisco Talos has identified UAT-8302, a China-linked espionage group actively targeting government networks across South America and southeastern Europe. The group abuses Microsoft cloud services, OneDrive and the MS Graph API, as command-and-control channels, making malicious traffic difficult to distinguish from normal enterprise activity. Post-compromise activity focuses on Active Directory and hybrid identity infrastructure, creating risk of credential theft, persistent access, and potential spillover to cloud-connected environments.

Technical Analysis

UAT-8302 is a China-nexus APT conducting long-term espionage operations against government entities, observed from late 2024 (South America) through 2025 (southeastern Europe). The group deploys NetDraft, CloudSorcerer v3, VSHELL, and SNOWLIGHT, malware families with documented overlap across at least six other tracked China-nexus clusters, indicating shared tooling infrastructure or direct operational coordination. Command-and-control is routed through Microsoft OneDrive and the MS Graph API (T1102.002, T1071.001), blending malicious traffic with legitimate cloud usage. Post-compromise activity targets Active Directory (T1482, T1069.002, T1087.002) and Azure AD Connect / Entra ID Connect (T1003, T1550.001, T1552.001), enabling

credential harvesting and hybrid identity persistence. Initial access and execution leverage Windows Command Shell and PowerShell (T1059.003, T1059.001). Lateral movement uses SMB/Windows Admin Shares (T1021.002) and valid accounts (T1078). DLL sideloading (T1574.002) and masquerading (T1036) are used for defense evasion. Relevant weaknesses: CWE-494 (Download of Code Without Integrity Check), CWE-312 (Cleartext Storage of Sensitive Information), CWE-522 (Insufficiently Protected Credentials). Note: CVE-2025-0994, referenced in preliminary source data, is a Trimble Cityworks deserialization vulnerability (CVSS 9.0) with no documented connection to this campaign and has been excluded from this report. Severity is assessed as High based on campaign characteristics, target profile, post-compromise scope, and EPSS percentile (0.98879). Source: Cisco Talos (https://blog.talosintelligence.com/uat-8302/).

Action Checklist

1. Containment, Audit Microsoft 365 and Azure AD audit logs immediately for anomalous OneDrive access patterns and MS Graph API calls originating from government endpoints; restrict MS Graph API access to approved applications via Conditional Access policies in Entra ID; isolate any endpoints exhibiting indicators associated with VSHELL, SNOWLIGHT, NetDraft, or CloudSorcerer v3.
2. Detection, Query Entra ID sign-in logs and Azure AD Connect sync logs for unexpected privileged sync account activity; review Windows Security Event logs for Event ID 4624 (logon) and 4648 (explicit credential use) on domain controllers and Azure AD Connect servers; hunt for DLL sideloading patterns (T1574.002) using EDR telemetry, focusing on MobaXterm process trees and unsigned DLLs loaded by trusted binaries; search for scheduled task creation (T1053.005) by non-standard accounts.
3. Eradication, Remove unauthorized scheduled tasks, DLL sideload artifacts, and any identified malware components (NetDraft, CloudSorcerer v3, VSHELL, SNOWLIGHT) from affected endpoints; reset credentials for all accounts with evidence of access by threat actor, prioritizing Azure AD Connect sync accounts and domain admin accounts; rotate secrets for any application registrations showing unauthorized MS Graph API consent.
4. Recovery, Validate Azure AD Connect / Entra ID Connect configuration integrity against known-good baseline; re-enable MFA enforcement for all privileged accounts and verify Conditional Access policy coverage; monitor Entra ID and on-premises AD for re-emergence of lateral movement indicators (T1021.002, T1078) for a minimum of 30 days post-remediation.
5. Post-Incident, Review cloud application consent policies to restrict MS Graph API delegated permissions to least-privilege; assess whether hybrid identity architecture (Azure AD Connect) introduces unacceptable lateral movement risk between on-premises and cloud environments; map identified TTPs against your detection coverage using MITRE ATT&CK navigator to identify blind spots in logging, alerting, and response playbooks.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior leadership, legal, and external IR retainer immediately if Azure AD Connect sync account compromise is confirmed, Azure AD tenant-level changes are detected (new Global Admin accounts, federated domain additions, or directory role assignments), or if any exfiltration of privileged credential material or PII from government endpoints is indicated — each condition triggers potential regulatory breach notification obligations and hybrid identity compromise requires tenant-level remediation authority beyond typical IR team scope.
Recovery Notes	After eradication of UAT-8302 artifacts and credential rotation, validate Azure AD Connect health by running a full delta sync (Start-ADSyncSyncCycle -PolicyType Delta) and reviewing the sync log for unexpected object changes or connector errors that may indicate a residual foothold in the hybrid identity pipeline. Re-enable and enforce MFA via Conditional Access for all accounts in the Directory Synchronization Accounts, Global Administrator, and Hybrid Identity Administrator roles before restoring any suspended services, as UAT-8302's primary persistence vector relies on accounts without MFA enforcement. Maintain enhanced logging on Entra ID sign-in activity, MS Graph API application consent events, and on-premises DC Security logs for a minimum of 30 days, given UAT-8302's demonstrated pattern of re-entry through previously compromised credentials after initial remediation.
Forensic Artifacts	Microsoft 365 Unified Audit Log — OneDrive FileAccessed and FileDownloaded operations with anomalous UserAgent strings or high-frequency access patterns from government endpoints, directly evidencing UAT-8302's use of OneDrive as a C2 staging channel | Entra ID Sign-In Logs — MS Graph API OAuth2 token issuance records showing appId, resourceDisplayName, and delegated permission scopes for unauthorized application registrations used by UAT-8302 to authenticate C2 callbacks through legitimate Microsoft infrastructure | Azure AD Connect trace logs at C:\ProgramData\AADConnect\ and Windows Security Event ID 4648 on the Azure AD Connect server — evidence of MSOL_ or AAD_ sync account credential abuse, which is UAT-8302's known path from on-premises AD compromise to Entra ID tenant-level access | MobaXterm installation directory DLL inventory (C:\Program Files (x86)\Mobatek\MobaXterm\) with file hashes compared against vendor-published manifest — unsigned or anomalous DLLs in this path are the primary artifacts of SNOWLIGHT and NetDraft delivery via T1574.002 DLL sideloading | Windows Registry export of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\ and corresponding Sysmon Event ID 1 process creation logs — captures the scheduled task persistence mechanism (T1053.005) used by UAT-8302, including encoded command lines, staging paths, and execution timestamps linking tasks to malware component activity

Per-Action IR Details

Containment — Audit Microsoft 365 and Azure AD audit logs immediately for anomalous OneDrive access patterns and MS Graph API calls originating from government endpoints; restrict MS Graph API access to approved applications via Conditional Access policies in Entra ID; isolate any endpoints exhibiting indicators associated with VSHELL, SNOWLIGHT, NetDraft, or CloudSorcerer v3.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-3 (Access Enforcement), NIST SI-4 (System Monitoring), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Without a SIEM, use Microsoft's free Unified Audit Log via PowerShell: Connect-ExchangeOnline, then run Search-UnifiedAuditLog -RecordType SharePointFileOperation -Operations FileDownloaded,FileAccessed filtering on UserAgent strings and IP addresses outside known government IP ranges. For MS Graph API abuse, query Entra ID sign-in logs via Microsoft Graph Explorer (free) filtering on appDisplayName eq 'Microsoft Graph' with resourceDisplayName containing 'OneDrive'. Isolate flagged endpoints immediately using Windows Firewall rules via

netsh advfirewall or Group Policy to block outbound 443 to Microsoft CDN ranges while preserving forensic state.

Evidence: Before containment, preserve: (1) Microsoft 365 Unified Audit Log exports filtered on OneDrive FileAccessed and FileDownloaded operations for the 90-day retention window — UAT-8302 uses OneDrive as a C2 staging area, so bulk download events from non-standard user agents are key indicators; (2) Entra ID sign-in logs showing MS Graph API OAuth token issuance to application registrations not in your approved app catalog — capture the appId, clientId, and resource fields; (3) Full memory image of any endpoint running MobaXterm at time of isolation, as SNOWLIGHT and NetDraft are delivered via DLL sideloading into MobaXterm process space; (4) Network capture (Wireshark on gateway) of TLS SNI fields to login.microsoftonline.com and graph.microsoft.com from affected endpoints to baseline normal vs. anomalous call frequency.

Detection — Query Entra ID sign-in logs and Azure AD Connect sync logs for unexpected privileged sync account activity; review Windows Security Event logs for Event ID 4624 (logon) and 4648 (explicit credential use) on domain controllers and Azure AD Connect servers; hunt for DLL sideloading patterns (T1574.002) using EDR telemetry, focusing on MobaXterm process trees and unsigned DLLs loaded by trusted binaries; search for scheduled task creation (T1053.005) by non-standard accounts.

NIST Phase: Detection Analysis

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

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

Compensating: Without EDR, deploy Sysmon (config: SwiftOnSecurity baseline minimum) and enable Event ID 7 (ImageLoaded) with signing status — filter for unsigned DLLs loaded by MobaXterm.exe (C:\Program Files (x86)\Mobatek\MobaXterm\). Query with: Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 7 -and $_.Message -match 'MobaXterm' -and $_.Message -match 'Signed: false'}. For scheduled task hunting (T1053.005), query Windows Security Event ID 4698 (scheduled task created) on all domain controllers: Get-WinEvent -LogName Security -FilterXPath '*[System[EventID=4698]]' | Select-Object TimeCreated, Message. For Azure AD Connect sync account abuse, extract MSOL_ or AAD_ prefixed account logons from DC Security logs using Event ID 4648 with SubjectUserName matching those patterns.

Evidence: Before completing detection sweeps, preserve: (1) Azure AD Connect server Application and System Event logs under C:\Windows\System32\winevt\Logs\ — UAT-8302 abuses the sync account's delegated rights, and Event ID 4648 with the MSOL_ sync account as SubjectUserName outside scheduled sync windows is a primary indicator; (2) Full Sysmon Event ID 1 (Process Create) logs showing MobaXterm.exe spawning child processes (cmd.exe, powershell.exe, or rundll32.exe) which is inconsistent with normal MobaXterm usage; (3) Windows Registry export of HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\ to capture scheduled task XML definitions including hidden or obfuscated command lines used by UAT-8302 for persistence (T1053.005); (4) Entra ID App Registration audit logs showing any OAuth2 permission grant events in the 30 days prior to detection.

Eradication — Remove unauthorized scheduled tasks, DLL sideload artifacts, and any identified malware components (NetDraft, CloudSorcerer v3, VSHELL, SNOWLIGHT) from affected endpoints; reset credentials for all accounts with evidence of access by threat actor, prioritizing Azure AD Connect sync accounts and domain admin accounts; rotate secrets for any application registrations showing unauthorized MS Graph API consent.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management), CIS 5.2 (Use Unique Passwords), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without enterprise credential management tooling, use the Microsoft free tool ADSIEdit or PowerShell to force-reset the MSOL_ or AAD_ sync account password: Set-ADAccountPassword -Identity 'MSOL_XXXXXXXXXX' -Reset -NewPassword (ConvertTo-SecureString -AsPlainText 'NewStrongPassword' -Force), then immediately re-sync via Azure AD Connect wizard. To remove unauthorized scheduled tasks identified in detection: schtasks /delete /tn 'TaskNameHere' /f on each affected endpoint. For DLL sideload artifact removal, verify MobaXterm installation

directory (C:\Program Files (x86)\Mobatek\MobaXterm\) against known-good file hashes from vendor and delete unsigned DLLs not matching. Rotate MS Graph API application secrets via Entra ID portal under App Registrations > Certificates & Secrets — remove all client secrets not created by your team and generate new ones.

Evidence: Before eradication begins, preserve full forensic images of: (1) The MobaXterm installation directory including all DLLs — SNOWLIGHT and NetDraft are DLL sideloads and the malicious DLL files are primary eradication targets; (2) The scheduled task XML definitions exported from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\ prior to deletion — these contain command-line arguments, encoded payloads, or staging paths used by UAT-8302 (T1053.005); (3) Prefetch files from C:\Windows\Prefetch\ for any executables launched from temp or user-writable directories indicating VSHELL or CloudSorcerer v3 staging activity; (4) Entra ID App Registration audit log showing the exact permissions granted to unauthorized app registrations before revocation — needed for post-incident assessment of data exposure scope.

Recovery — Validate Azure AD Connect / Entra ID Connect configuration integrity against known-good baseline; re-enable MFA enforcement for all privileged accounts and verify Conditional Access policy coverage; monitor Entra ID and on-premises AD for re-emergence of lateral movement indicators (T1021.002, T1078) for a minimum of 30 days post-remediation.

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 AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Without a commercial PAM or monitoring solution, use the free Microsoft Entra ID Workbooks (built into the Azure portal at no extra cost for P1 tenants) to create a persistent alert on sign-ins by accounts in the Global Administrator, Hybrid Identity Administrator, or Directory Synchronization Accounts roles from new locations or devices. For on-premises AD lateral movement (T1021.002 — SMB/Windows Admin Shares), enable Windows Security Event ID 5140 (network share accessed) auditing on DCs and file servers and alert on ADMIN$ or C$ access from non-admin workstations. Validate Azure AD Connect configuration integrity by running: Import-Module ADSync; Get-ADSyncScheduler and comparing connector account assignments against your pre-incident documentation.

Evidence: During recovery monitoring, continuously collect: (1) Entra ID sign-in logs filtered on the reset MSOL_ sync account and any new service principal activity — re-appearance of Graph API calls from these identities indicates reinfection or a missed persistence mechanism; (2) Windows Security Event ID 4624 logon Type 3 (network) and Type 10 (remote interactive) on domain controllers for accounts flagged during eradication, which would indicate UAT-8302 retained an undiscovered credential (T1078 — Valid Accounts); (3) SMB connection logs (Event ID 5140) on high-value servers for lateral movement using pass-the-hash or stolen Kerberos tickets consistent with T1021.002, which is UAT-8302's known post-compromise pivot technique.

Post-Incident — Review cloud application consent policies to restrict MS Graph API delegated permissions to least-privilege; assess whether hybrid identity architecture (Azure AD Connect) introduces unacceptable lateral movement risk between on-premises and cloud environments; map identified TTPs against your detection coverage using MITRE ATT&CK navigator to identify blind spots in logging, alerting, and response playbooks.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AC-6 (Least Privilege), NIST CM-6 (Configuration Settings), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Without a threat intelligence platform, use the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to manually annotate UAT-8302 TTPs confirmed in this incident: T1574.002 (DLL Sideloading via MobaXterm), T1053.005 (Scheduled Task persistence), T1078 (Valid Accounts — MSOL_ sync account), T1021.002 (SMB lateral movement), and T1102 (Web Service C2 via OneDrive/MS Graph). For hybrid identity risk assessment, run the free Microsoft tool AADInternals (PowerShell module) in a test environment

to enumerate pass-through authentication agents and AD Connect connector accounts to identify the attack surface UAT-8302 exploited. Document app consent policy changes using Entra ID's built-in Permissions & Consent settings under Enterprise Applications — restrict user consent to verified publishers only.

Evidence: For the post-incident review, compile: (1) The full timeline of UAT-8302 MS Graph API OAuth token issuance events from Entra ID logs, showing which delegated permissions (Mail.Read, Files.ReadWrite, Directory.Read.All) were abused — this directly informs which API permission scopes must be restricted in the consent policy redesign; (2) The Azure AD Connect audit log showing all synchronization events during the compromise window, available at C:\ProgramData\AADConnect\ in trace log format, to determine whether the sync account was used to push unauthorized objects or attribute changes to Entra ID; (3) A completed ATT&CK Navigator layer file (.json) documenting which UAT-8302 techniques were detected by existing controls vs. those only discovered through manual investigation — this is the primary deliverable for the detection gap assessment.

Detection Guidance

Primary detection surfaces: (1) Microsoft 365 / Entra ID audit logs, look for MS Graph API calls from unexpected source IPs or service principals, particularly to OneDrive endpoints outside normal business hours or from government-network IP ranges not associated with approved cloud workflows (T1102.002, T1567.002); (2) Azure AD Connect server logs, monitor for unexpected sync account logins, password hash sync anomalies, and configuration changes; (3) Windows Security Event logs on domain controllers, Event IDs 4728, 4732, 4756 (group membership changes), 4769 (Kerberos service ticket requests at high volume, T1558), 4776 (NTLM authentication); (4) EDR/endpoint telemetry, hunt for MobaXterm spawning unexpected child processes, unsigned DLLs loaded via sideloading (T1574.002), and PowerShell or cmd.exe executing encoded or obfuscated commands (T1059.001, T1059.003, T1027); (5) Network, look for recurring HTTPS connections to OneDrive/Graph API endpoints at regular intervals from hosts that do not normally use these services (C2 beaconing pattern). Behavioral indicators: privilege enumeration via net group commands (T1069.002, T1087.002), network scanning activity (T1046), and archive creation preceding data movement (T1560, T1560.001). No public IOC list was available at time of writing, monitor Cisco Talos threat intelligence feeds for updated indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not publicly disclosed at time of writing`	Cisco Talos report did not publish specific IOCs in the source reviewed; monitor Talos threat intelligence feeds for updates	LOW

Framework Mappings

MITRE-ATTACK

- **T1059.003** — Windows Command Shell
- **T1078** — Valid Accounts
- **T1567.002** — Exfiltration to Cloud Storage
- **T1059.001** — PowerShell

- **T1560** — Archive Collected Data
- **T1053.005** — Scheduled Task
- **T1046** — Network Service Discovery
- **T1021.002** — SMB/Windows Admin Shares
- **T1059** — Command and Scripting Interpreter
- **T1069.002** — Domain Groups
- **T1550.001** — Application Access Token
- **T1552.001** — Credentials In Files
- **T1071.001** — Web Protocols
- **T1016** — System Network Configuration Discovery
- **T1083** — File and Directory Discovery
- **T1102.002** — Bidirectional Communication
- **T1047** — Windows Management Instrumentation
- **T1036** — Masquerading
- **T1087.002** — Domain Account
- **T1003** — OS Credential Dumping
- **T1027** — Obfuscated Files or Information
- **T1560.001** — Archive via Utility
- **T1018** — Remote System Discovery
- **T1555** — Credentials from Password Stores
- **T1574.002** — DLL Side-Loading
- **T1482** — Domain Trust Discovery
- **T1105** — Ingress Tool Transfer
- **T1057** — Process Discovery

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059.003	Windows Command Shell	Execution
T1078	Valid Accounts	Defense-Evasion
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1059.001	PowerShell	Execution
T1560	Archive Collected Data	Collection
T1053.005	Scheduled Task	Execution
T1046	Network Service Discovery	Discovery
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1059	Command and Scripting Interpreter	Execution
T1069.002	Domain Groups	Discovery
T1550.001	Application Access Token	Defense-Evasion
T1552.001	Credentials In Files	Credential-Access
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1016	System Network Configuration Discovery	Discovery
T1083	File and Directory Discovery	Discovery
T1102.002	Bidirectional Communication	Command-And-Control
T1047	Windows Management Instrumentation	Execution
T1036	Masquerading	Defense-Evasion
T1087.002	Domain Account	Discovery
T1003	OS Credential Dumping	Credential-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1560.001	Archive via Utility	Collection
T1018	Remote System Discovery	Discovery
T1555	Credentials from Password Stores	Credential-Access
T1574.002	DLL Side-Loading	Persistence
T1482	Domain Trust Discovery	Discovery
T1105	Ingress Tool Transfer	Command-And-Control
T1057	Process Discovery	Discovery

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/uat-8302/	T3
CVE-2025-0994 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-0994	T1
Vulnerability Details : CVE-2025-0994 - Cityworks	https://www.cvedetails.com/cve/CVE-2025-0994/	T3
Trimble Cityworks: CVE-2025-0994: Active Exploitation	https://www.recordedfuture.com/blog/trimble-cityworks-cve-2025-0994...	T3
CVE-2025-0994 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2025-0994	T3

Source	URL	Tier
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-0994	**T1**

Generated 2026-05-05 08:36 UTC by TJS Security Command Center